

SECURITY POLICIES.

Table of Contents

<i>Acceptable Use Policy</i>	42
I. Overview	42
II. Purpose	42
III. Scope	42
IV. Policy	42
A. INFORMATION ACCESS, CONTENT, AND USE	43
B. PROTECTING CONFIDENTIAL INFORMATION	44
C. COPYRIGHTED INFORMATION	45
D. PRIVACY STATEMENT	46
E. MONITORING AND INSPECTING INFORMATION SYSTEMS	46
F. STORING AND ARCHIVING INFORMATION	48
G. EMPLOYEE USAGE	48
H. INFORMATION SYSTEMS AWARENESS	49
I. ELECTRONIC MAIL (E-MAIL) AND ETIQUETTE	50
J. SECURING INFORMATION SYSTEMS WITH PASSWORDS	52
K. PROTECTING INFORMATION SYSTEMS	53
L. ENCRYPTING DATA	53
M. SECURING MOBILE COMPUTING DEVICES	53
N. ACCEPTABLE USE	54
O. UNACCEPTABLE USE	54
V. Enforcement	55
VI. Distribution	55
<i>Access Control Policy</i>	56
I. Overview	56
II. Purpose	56
III. Scope	56
IV. Policy	56
V. Enforcement	58
VI. Distribution	58
<i>Account Management Policy</i>	60
I. Overview	60
II. Purpose	60
III. Scope	60
IV. Policy	60
V. Enforcement	65

VI. Distribution	66
<i>Acquisition and Procurement Policy</i>	<i>67</i>
I. Overview	67
II. Purpose	67
III. Scope	67
IV. Policy	67
A. PROCUREMENT ACTION	68
B. REVIEW	69
C. ACQUISITION STRATEGY	69
D. DATA COLLECTION REQUIREMENTS	70
E. IT PRODUCTS AND SERVICES	71
V. Enforcement	72
VI. Distribution	73
<i>Admin Special Access Policy</i>	<i>74</i>
I. Overview	74
II. Purpose	74
III. Scope	74
IV. Policy	74
V. Enforcement	75
VI. Distribution	75
<i>Agreement : Business Associate Agreement</i>	<i>77</i>
<i>Agreement : Non-Disclosure Agreement</i>	<i>82</i>
<i>Anti-Malware Policy</i>	<i>84</i>
I. Overview	84
II. Purpose	84
III. Scope	84
IV. Policy	84
V. Enforcement	86
VI. Distribution	86
<i>Application Implementation Policy</i>	<i>87</i>
I. Overview	87
II. Purpose	87
III. Scope	87

IV. Policy.....	87
V. Enforcement	88
VI. Distribution	88
<i>Approved Application Policy</i>	<i>90</i>
I. Overview	90
II. Purpose	90
III. Scope.....	90
IV. Policy.....	90
V. Enforcement	91
VI. Distribution	91
<i>Asset Management Policy</i>	<i>93</i>
I. Overview	93
II. Purpose	93
III. Scope.....	93
IV. Policy.....	93
A. ASSET TYPES	93
B. ASSET VALUE	94
C. ASSET MEDIA.....	94
D. ASSET TRACKING REQUIREMENTS.....	95
E. TRANSFER PROCEDURE	95
F. ASSET TRANSFERS	96
G. ASSET DISPOSAL AND REPURPOSING	96
H. MEDIA USE	97
I. SEPARATION OF DUTIES.....	97
J. CLEARING AND SANITATION	97
K. PROTECTION MEASURES.....	97
V. Enforcement.....	98
VI. Distribution	98
<i>Audit Policy</i>	<i>100</i>
I. Overview	100
II. Purpose	100
III. Scope.....	100
IV. Policy.....	100
V. Enforcement	102
VI. Distribution	102

Audit Trails Policy	104
I. Overview	104
II. Purpose	104
III. Scope.....	104
IV. Policy.....	104
A. PURPOSE	104
B. AUDIT TRAIL REQUIREMENTS	105
C. REVIEW AND ANALYSIS.....	106
D. SECURITY CONSIDERATIONS.....	107
V. Enforcement	108
VI. Distribution	108
Backup Plan	109
I. Purpose of the Backup Plan	109
II. Overview of the Backup Plan	109
III. Business Continuity Objectives	110
IV. Responsibilities.....	111
V. Backup Procedures	112
A. OVERVIEW	112
B. ARCHIVING AND RETENTION	112
C. OFF-SITE STORAGE	113
D. DISPOSAL PROCEDURES	113
E. TESTING BACKUPS	114
VI. Storage of Backups.....	115
A. ON-SITE BACKUPS	115
B. OFF-SITE BACKUPS	115
Exhibit A – Archiving and Rotation Schedule	116
Backup Policy	117
I. Overview	117
II. Purpose	117
III. Scope.....	117
IV. Policy.....	117
V. Enforcement	120
VI. Distribution	120
Bluetooth Policy	121
I. Overview	121

II. Purpose	121
III. Scope	121
IV. Policy	121
A. DEVICES	121
B. SECURITY	121
C. USER RESPONSIBILITIES	122
V. Enforcement	122
VI. Distribution	122
<i>Bring Your Own Device And Technology Policy.....</i>	<i>124</i>
I. Overview	124
II. Purpose	124
III. Scope	124
IV. Policy	124
V. Enforcement	127
VI. Distribution	127
<i>Business Continuity Business Resumption Plan.....</i>	<i>129</i>
I. Purpose of the Business Resumption Plan	129
II. Overview of the Business Resumption Plan	129
III. Preparing For A Disaster	130
A. INFORMATION NEEDED BEFORE A DISASTER	130
B. INFORMATION NEEDED DURING A DISASTER.....	130
IV. Disaster	132
A. DISASTER NOTIFICATION	132
B. ADMINISTRATIVE TEAM	132
C. USER DEPARTMENT RESPONSIBILITIES.....	132
V. Procedures for Returning to Normal Operations	134
A. EMERGENCY ACTION TEAM PROCEDURES	134
B. USER DEPARTMENT PROCEDURES.....	134
VI. After a Disaster	135
Appendix A – Distribution List	135
Appendix B – Receipt and Acknowledgement	136
<i>Business Continuity Disaster Recovery Plan.....</i>	<i>137</i>
I. Purpose of the Business Continuity Disaster Recovery Plan	137
II. Business Continuity Philosophy	137
III. Policy Statement	137

IV. Overview of the Plan.....	138
V. Example Recovery Scenarios.....	139
A. Three phases of recovery	139
B. Example #1 - partial interruption of services (minor severity)	139
C. Example #2 - major failure but network intact (moderate severity)	140
D. EXAMPLE #3 – CENTRAL NETWORK AND OFFICES DESTROYED (MAJOR SEVERITY).....	141
VI. The Readiness Team.....	142
A. Purpose of the readiness team	142
B. Organizing and planning	142
C. Emergency coordinator	143
D. Alternate emergency coordinator	144
E. Contingency site coordinator	144
F. Use of emergency action teams	145
G. Emergency control center	145
VII. Major Services, Users, and Key Considerations.....	146
A. Purpose of major services, users, and key considerations	146
C. External services and applications	147
D. Information systems equipment considerations	148
E. Special considerations	148
VIII. General Procedures for Potential Interruptions.....	149
A. Purpose of general procedures for potential interruptions	149
B. Recovery plan for fires	149
C. Recovery Plan For Electrical Outages	151
D. Recovery plan for telecommunications failures	151
E. Recovery plan for flooding	152
F. Recovery plan for hardware failures	153
G. Recovery plan for software failures.....	154
IX. Policies For Reducing Risks	155
A. Protecting data.....	155
B. Backup procedures.....	155
C. Backup storage procedures.....	155
D. Protecting network servers.....	155
E. Protecting vital records	156
F. Backup of data, hardware, supplies & documentation	156
G. Insurance	156
X. Contingency Site Description	157
A. Emergencies and disasters.....	157
B. Contingency site space and resource requirements	157
C. Recovery plan testing.....	157
XI. Emergency Action Teams.....	158
A. Responsibilities of the emergency action teams	158
B. Emergency action operations team	158
C. Emergency action applications team	159
D. Emergency action hardware team.....	159
E. Emergency action facilities team	160

F. Emergency action administrative assistance team	160
XII. Procedures for an Emergency or Disaster	161
A. Notifying the readiness team.....	161
B. Initial readiness team procedures.....	161
C. Activating the emergency control center.....	162
D. Notifying action teams and company management.....	163
E. Notification of offsite storage and contingency sites.....	163
F. Summary of procedures for recovery operations	164
G. Initial procedures at contingency site.....	165
H. Initial procedures at offsite storage site	165
I. Pickup of backup materials by emergency action operations team	165
J. Assembling and coordinating of all emergency teams	166
K. Activating contingency site by emergency action operations team	167
L. Recovering lost work by emergency action applications team	168
M. Coordinating users by emergency action applications team	169
N. Hardware salvage or replacing by emergency action hardware team	170
O. Facilities salvage or replacing by emergency action facilities team	170
P. Administrative coordinating by administrative team	171
Q. Specific procedures for user department contingencies.....	171
R. Operating of application systems.....	172
S. Procedures for replacing network server room	172
T. Procedures for returning to normal operations.....	173
XIII. Testing and Maintaining the Plan.....	174
A. Policies and procedures for testing.....	174
B. Policies and procedures for review and update.....	175
XIV. Appendices	176
<i>Business Continuity of Operations.....</i>	<i>185</i>
<i>Department Plan</i>	<i>185</i>
I. Purpose of the Business Continuity of Operations Department Plan	185
II. Overview of the Business Continuity of Operations Department Plan	185
III. Department Description	186
IV. Preparing For A Disruption	186
A. IMPORTANT SERVICES AND PROCESSES	186
B. IMPORTANT RESOURCES	186
C. DEPARTMENT DEPENDENCIES	187
D. DEPARTMENT LEADERSHIP SUCCESSION	187
E. SPECIAL CONSIDERATIONS	187
V. Disruption.....	187
A. NOTIFICATION.....	187
B. INITIAL RESPONSE	187
C. GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS	188
D. DISRUPTION PROCEDURES	188
E. RECOVERY STEPS.....	188

F. PLAN TESTING AND UPDATES	189
Appendix A – Distribution List	189
Appendix B – Receipt and Acknowledgement	190
<i>Business Continuity Plan</i>	<i>191</i>
I. Purpose of the Business Continuity Plan	191
II. Overview of the Business Continuity Plan	191
III. Business Continuity Policy	192
IV. Business Impact Analysis	192
V. Business Continuity Disaster Recovery Plan	193
VI. Business Continuity Business Resumption Plan	194
VII. Business Continuity Communications Plan	195
VIII. Business Continuity Operations Plan.....	196
Appendix A – Distribution List	197
Appendix B – Receipt and Acknowledgement	197
<i>Business Continuity Policy.....</i>	<i>198</i>
I. Overview	198
II. Purpose	198
III. Scope	198
IV. Policy.....	198
V. Enforcement	200
VI. Distribution	201
<i>Business Impact Analysis</i>	<i>202</i>
I. Introduction.....	202
A. PURPOSE	202
B. SCOPE	202
C. SUPPORTING INFORMATION	203
II. Business Processes	203
A. OVERVIEW	203
B. IMPORTANCE.....	203
III. Financial Impact	204
B. FINANCIAL IMPLICATIONS	205
IV. Non-Financial Impacts	205
A. OVERVIEW	205
B. NON-FINANCIAL IMPLICATIONS	206

V. Manual Procedures	206
A. OVERVIEW	206
B. BUSINESS CONTINUITY	206
VI. Work Area Requirements	207
A. OVERVIEW	207
B. DEPARTMENT REQUIREMENTS	207
VII. Application Software.....	208
A. OVERVIEW	208
B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES	208
VIII. Third Party Services.....	209
A. OVERVIEW	209
B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES	209
VIII. Information Technology	210
A. OVERVIEW	210
B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES	210
IX. Summary	211
A. OVERVIEW	211
B. IT ALIGNMENT	211
C. DEPARTMENT RESPONSIBILITIES	212
<i>Capacity and Utilization Policy.....</i>	<i>214</i>
I. Overview	214
II. Purpose	214
III. Scope.....	214
IV. Policy.....	214
V. Enforcement	216
VI. Distribution	216
<i>Certification and Accreditation Policy</i>	<i>217</i>
I. Overview	217
II. Purpose	217
III. Scope.....	217
IV. Policy.....	217
V. Enforcement	219
VI. Distribution	219
<i>Change Management Policy</i>	<i>220</i>
I. Overview	220
II. Purpose	220

III. Scope.....	220
IV. Policy.....	220
V. Enforcement.....	221
VI. Distribution	221
<i>Clear Desk Policy</i>	223
I. Overview	223
II. Purpose	223
III. Scope.....	223
IV. Policy.....	223
V. Enforcement.....	224
VI. Distribution	224
<i>Cloud Service Provider Policy</i>	226
I. Overview	226
II. Purpose	226
III. Scope.....	226
IV. Policy.....	226
V. Enforcement.....	229
VI. Distribution	229
<i>Compliance Policy.....</i>	230
I. Overview	230
II. Purpose	230
III. Scope.....	230
IV. Policy.....	230
V. Enforcement.....	232
VI. Distribution	232
<i>Configuration Management Plan.....</i>	233
I. Introduction.....	233
II. Purpose of the Configuration Management Plan	233
III. Roles and Responsibilities.....	234
A. INTRODUCTION	234
B. CONFIGURATION MANAGEMENT COMMITTEE.....	234
C. CONFIGURATION ITEMS.....	234

D. BASELINE CONFIGURATIONS	234
IV. Configuration Control.....	235
A. PROCESS OVERVIEW	235
B. APPROVED CHANGE REQUESTS	235
V. Configuration Management.....	236
A. OVERVIEW	236
B. CONFIGURATION MANAGEMENT DATABASE	236
C. CONFIGURATION STATUS ACCOUNTING.....	236
VI. Configuration Management Audits	237
A. AUDIT PROCESS	237
C. AUDIT REPORT	238
Appendix A – Distribution List	238
Appendix B – Receipt and Acknowledgement	239
<i>Configuration Management Policy.....</i>	<i>240</i>
I. Overview	240
II. Purpose	240
III. Scope	240
IV. Policy.....	240
A. RISK MANAGEMENT	240
B. CONFIGURATION MANAGEMENT PROCESSES	240
C. CONFIGURATION MANAGEMENT CHANGE CONTROL.....	241
D. SECURITY/PRIVACY IMPACT ANALYSIS	242
E. CONFIGURATION SETTINGS	242
F. CONFIGURATION MANAGEMENT PLAN.....	242
V. Enforcement	243
VI. Distribution	243
<i>Context and Alignment Policy.....</i>	<i>244</i>
I. Overview	244
II. Purpose	244
III. Scope	244
IV. Policy.....	244
V. Enforcement	245
VI. Distribution	245
<i>COVID-19 Response Policy</i>	<i>247</i>
I. Overview	247
II. Purpose	247

III. Scope.....	247
IV. Policy.....	247
V. Enforcement.....	248
VI. Distribution	248
<i>Cybersecurity Framework Policy</i>	250
I. Overview	250
II. Purpose	250
III. Scope.....	250
IV. Policy.....	250
A. CYBERSECURITY FRAMEWORK FUNCTIONS.....	250
B. CYBERSECURITY FRAMEWORK IMPLEMENTATION.....	253
C. CYBERSECURITY FRAMEWORK PROFILE.....	255
V. Enforcement.....	255
VI. Distribution	255
<i>Cybersecurity Policy.....</i>	257
I. Overview	257
II. Purpose	257
III. Scope.....	257
IV. Policy.....	257
A. FUNCTIONS.....	258
B. IMPLEMENTATION TIERS.....	258
C. PROFILES	259
D. CYBERSECURITY FRAMEWORK	259
V. Enforcement.....	263
VI. Distribution	263
<i>Data Analytics Policy</i>	265
I. Overview	265
II. Purpose	265
III. Scope.....	265
IV. Policy.....	265
A. BACKGROUND	265
B. SECURITY CONTROLS.....	266
V. Enforcement.....	267
VI. Distribution	267

<i>Data Classification Policy</i>	269
I. Overview	269
II. Purpose	269
III. Scope	269
IV. Policy	269
V. Enforcement	270
VI. Distribution	270
<i>Data Integrity Policy</i>	272
I. Overview	272
II. Purpose	272
III. Scope	272
IV. Policy	272
V. Enforcement	273
VI. Distribution	273
<i>Data Marking Policy</i>	274
I. Overview	274
II. Purpose	274
III. Scope	274
IV. Policy	274
A. GENERAL	275
B. IDENTIFICATION MARKINGS	275
C. INADVERTENT RELEASE	276
D. RESPONSIBILITIES	276
V. Enforcement	278
VI. Distribution	278
<i>Data Privacy Policy</i>	279
I. Overview	279
II. Purpose	279
III. Scope	279
IV. Policy	279
A. NETWORK DATA	279
B. EXCEPTIONS	280
C. REQUESTS FOR NETWORK DATA	280
V. Enforcement	280

VI. Distribution	281
<i>Data Retention Policy</i>	282
I. Overview	282
II. Purpose	282
III. Scope	282
IV. Policy	282
A. RESPONSIBILITIES	282
B. RETENTION REQUIREMENTS	283
C. RETENTION RESOURCES	284
V. Enforcement	286
VI. Distribution	286
<i>Database Security Policy</i>	288
I. Overview	288
II. Purpose	288
III. Scope	288
IV. Policy	288
A. Access	288
B. Security Protection	288
V. Enforcement	289
VI. Distribution	289
<i>Disposal Policy</i>	291
I. Overview	291
II. Purpose	291
III. Scope	292
IV. Policy	292
V. Enforcement	293
VI. Distribution	293
<i>Documentation Policy</i>	294
I. Overview	294
II. Purpose	294
III. Scope	294
IV. Policy	294
A. RESPONSIBILITIES	294
B. NETWORK DOCUMENTATION	295

C. DOCUMENTATION ACCESS	295
D. DOCUMENTATION REVIEW	296
E. DOCUMENTATION STORAGE.....	296
V. Enforcement	296
VI. Distribution	296
<i>Domain Controller Policy</i>	<i>297</i>
I. Overview	297
II. Purpose	297
III. Scope.....	297
IV. Policy.....	297
V. Enforcement.....	298
VI. Distribution	298
<i>Domain Name System Policy.....</i>	<i>299</i>
I. Overview	299
II. Purpose	299
III. Scope.....	299
IV. Policy.....	299
V. Enforcement.....	300
VI. Distribution	300
<i>E-Commerce Policy</i>	<i>301</i>
I. Overview	301
II. Purpose	301
III. Scope.....	301
IV. Policy.....	301
V. Enforcement.....	302
VI. Distribution	302
<i>E-Mail Policy</i>	<i>303</i>
I. Overview	303
II. Purpose	303
III. Scope.....	303
IV. Policy.....	303
A. COMPANY USES OF E-MAIL	303

B. FORWARDING OF E-MAIL MESSAGES	303
C. SECURITY AND PRIVACY	304
D. E-MAIL RETENTION	304
E. ENCRYPTED COMMUNICATIONS.....	305
V. Enforcement	305
VI. Distribution	305
<i>Encryption Policy</i>	<i>307</i>
I. Overview	307
II. Purpose	307
III. Scope.....	307
IV. Policy.....	307
A. KEY LENGTHS	308
B. DATA AT REST	308
C. PORTABLE DEVICES	309
D. TRANSMISSION SECURITY	310
E. ENCRYPTION KEY MANAGEMENT	311
F. ENCRYPTION OF DATA	313
V. Enforcement	313
VI. Distribution	313
<i>Ethics Policy.....</i>	<i>314</i>
I. Overview	314
II. Purpose	314
III. Scope.....	314
IV. Policy.....	314
V. Enforcement	315
VI. Distribution	315
<i>EU Privacy and Data Protection Policy</i>	<i>317</i>
I. Overview	317
II. Purpose	317
III. Scope.....	317
IV. Policy.....	317
A. PRIVACY PRINCIPLES	317
B. DATA PROTECTION	320
V. Enforcement	321
VI. Distribution	321

Facility Security Plan.....	322
I. Introduction.....	322
A. Overview	322
B. Risk Assessment	322
C. Equipment.....	322
D. Plan Updates.....	322
II. Facility Overview.....	323
A. Facility Information	323
B. Business Operations.....	323
C. Documentation	323
III. Personnel Considerations	323
A. Overview	323
B. Personnel Controls.....	323
C. Security Controls	324
D. Mailing Handling.....	324
E. Drills	325
IV. Equipment Considerations	326
A. Overview.....	326
B. Equipment Controls	326
C. Disaster Controls	326
V. Environmental Considerations.....	327
A. Overview	327
B. Power Controls.....	327
C. Heating and Air Conditioning System Controls.....	328
D. Water Controls.....	328
VI. Cabling Considerations.....	328
A. Overview	328
B. Power and Telecommunications Controls	328
C. Sensitive or Critical Systems.....	329
VII. Maintenance Considerations	329
A. Overview	329
B. Frequency	329
C. Maintenance Controls.....	329
VIII. Off-site Considerations.....	330
A. Overview	330
B. Off-site Controls	330
IX. Equipment Disposal/Re-use Considerations	330
A. Overview	330
B. Disposal/Re-use Controls	330
Appendix A – Supporting Documents.....	331
Appendix B – Receipt and Acknowledgement	332
Firewall Hardening Procedure.....	333

I. Overview	333
II. Purpose	333
III. Scope	333
IV. Procedure	333
V. Enforcement	335
VI. Distribution	335
<i>Firewall Policy</i>	<i>336</i>
I. Overview	336
II. Purpose	336
III. Scope	336
IV. Policy	336
V. Enforcement	339
VI. Distribution	340
<i>Forms</i>	<i>341</i>
Asset Transfer Form	342
Audit Log Form	343
Backup Log Form	344
Business Impact Analysis Questionnaire Form	345
Change Management Log Form	347
Incident Response Form	348
Information Systems Access Request Form	349
Information Systems Log Form	350
Problem Management Form	351
Third Party Service Provider Log Form	352
<i>GDPR EU Privacy and Data Protection Policy</i>	<i>353</i>
I. Overview	353
II. Purpose	353
III. Scope	353
IV. Policy	353
A. PRIVACY PRINCIPLES	353
B. DATA PROTECTION OFFICER	356
C. DATA PROTECTION TECHNICAL AND ORGANIZATIONAL MEASURES	356

D. DATA PROTECTION IMPACT ASSESSMENT	357
V. Enforcement	358
VI. Distribution	358
<i>Green Computing Policy</i>	<i>360</i>
I. Overview	360
II. Purpose	360
III. Scope	360
IV. Policy	360
A. DESKTOP (PERSONAL) COMPUTER USAGE AND MANAGEMENT	360
B. SHARED-USE OFFICE DEVICES	361
C. IT DEPARTMENT	361
D. PURCHASING DEPARTMENT	362
E. EQUIPMENT RECLAMATION, RECYCLING, AND DISPOSAL	363
V. Enforcement	363
VI. Distribution	363
<i>Guest Access Policy</i>	<i>365</i>
I. Overview	365
II. Purpose	365
III. Scope	365
IV. Policy	365
V. Enforcement	367
VI. Distribution	367
<i>Hardware and Software Maintenance Policy</i>	<i>369</i>
I. Overview	369
II. Purpose	369
III. Scope	369
IV. Policy	369
A. HARDWARE	369
B. SOFTWARE	370
C. APPROVAL	371
V. Enforcement	371
VI. Distribution	371
<i>Health Safety Policy</i>	<i>372</i>
I. Overview	372

II. Purpose	372
III. Scope.....	372
IV. Policy.....	372
A. HEALTH SAFETY OVERVIEW	372
B. ENTRY AREAS.....	373
C. PROTECTIVE EQUIPMENT.....	373
D. HEALTH SAFETY REMINDERS.....	373
E. SAFETY PRECAUTIONS	373
F. PHYSICAL DISTANCING.....	374
G. SANITIZING PROCEDURES	374
H. WORK ENVIRONMENTS.....	374
V. Enforcement.....	374
VI. Distribution	374
<i>HIPAA and HITECH Policy.....</i>	<i>376</i>
I. Overview	376
II. Purpose	376
III. Scope.....	376
IV. Policy.....	376
V. Enforcement.....	379
VI. Distribution	379
<i>HITRUST Policy</i>	<i>380</i>
I. Overview	380
II. Purpose	380
III. Scope.....	380
IV. Policy.....	380
V. Enforcement.....	384
VI. Distribution	384
<i>Identification and Authentication Policy</i>	<i>386</i>
I. Overview	386
II. Purpose	386
III. Scope.....	386
IV. Policy.....	386
V. Enforcement.....	388
VI. Distribution	388

Identity Theft Protection Policy.....	390
I. Overview	390
II. Purpose	390
III. Scope.....	390
IV. Policy.....	390
A. PROGRAM COORDINATOR	390
B. EMPLOYEE MANAGEMENT AND TRAINING	392
C. OBTAINING CUSTOMER INFORMATION AND VERIFYING CUSTOMER IDENTITIES	393
D. INFORMATION SYSTEMS	394
E. SELECTION AND OVERSIGHT OF SERVICE PROVIDERS	395
F. IDENTITY THEFT DETECTION	396
G. IDENTITY THEFT RESPONSE PROCEDURES	397
V. Enforcement	398
VI. Distribution	398
Incident Response Plan	399
I. Introduction.....	399
II. Incident Response Team.....	399
A. Incident Response Team Members	400
B. Incident Response Team Roles and Responsibilities.....	400
III. Incident Response Team Notification.....	402
A. Examples of Incidents	402
B. Risk Assessment Classification	403
C. Incident Declaration	403
IV. Response Procedures	403
A. Incident Response Phases.....	403
B. Issues.....	405
V. Breach of Information Security.....	405
A. Overview	405
B. Security Breach	406
C. Data Owner Responsibilities	406
D. Location Manager Responsibilities	407
E. When Notification Is Required	407
Appendix A - Incident Response Notification	408
A. Escalation.....	408
B. Internal Contact Auxiliary Members (as needed)	408
C. External Contacts (as needed)	408
D. Notification Order	408
Appendix B - Incident Response Team Members.....	409
Appendix C - Legislation	410
A. U.S. Security Breach/Breach Notification Laws	410

B. Gramm-Leach-Bliley Act (GLBA).....	411
C. Health Insurance Portability and Accountability Act (HIPAA)	412
D. Health Information Technology for Economic and Clinical Health (HITECH) Act	413
E. General Data Protection Regulation (GDPR)	413
Appendix D - Payment Card Standards.....	415
A. Requirements.....	415
B. On-site reviews	415
C. Self-Assessments.....	415
D. PCI Data Security Standard Plan	415
E. MasterCard Specific Steps.....	416
F. Visa U.S.A. Specific Steps.....	416
G. Steps and Requirements for Compromised Entities.....	417
H. Steps for Merchant Banks.....	418
I. Forensic Investigation Guidelines	418
J. Visa Incident Report Template.....	419
K. Discover Card Specific Steps	420
L. American Express Specific Steps.....	420
Appendix E - Incident Response Team Procedures	420
A. IT Operations Team.....	421
B. Chief Security Officer (MGMT).....	421
C. Information Privacy Team	424
D. Network Architecture Team	424
E. Operating System Architecture Team	424
F. Business Applications Team	426
G. Online Sales Team	426
H. Internal Audit Team	427
I. Customer Database Team	427
J. Credit Payment Systems Team	428
K. Legal Team	429
L. Human Resources Team	430
M. Public Relations Team.....	430
N. Location Manager Team	431
Appendix F - Security Breach/Data Breach Resources.....	432
A. Data Breach Notification and Response Services	432
B. Credit/Monitoring Services	432
Appendix G – Receipt and Acknowledgement	433
<i>Incident Response Policy.....</i>	<i>434</i>
I. Overview	434
II. Purpose	434
III. Scope.....	434
IV. Policy.....	434
A. ESTABLISHMENT OF AN INCIDENT RESPONSE TEAM	435
B. IDENTIFYING AND REPORTING INCIDENTS	436
C. RISK ASSESSMENT CLASSIFICATION	436

D. DOCUMENTATION AND COMMUNICATION OF INCIDENTS	437
E. RESPONDER PROCEDURES	437
F. SPECIAL SITUATIONS/EXCEPTIONS	438
G. INCIDENT REPORTING	438
H. TRAINING	438
V. Enforcement	439
VI. Distribution	439
<i>Internet Connection Policy</i>	<i>440</i>
I. Overview	440
II. Purpose	440
III. Scope	440
IV. Policy	441
V. Enforcement	441
VI. Distribution	442
<i>Intrusion Detection Policy</i>	<i>443</i>
I. Overview	443
II. Purpose	443
III. Scope	443
IV. Policy	443
V. Enforcement	445
VI. Distribution	445
<i>IT Governance Policy</i>	<i>447</i>
I. Overview	447
II. Purpose	447
III. Scope	447
IV. Policy	447
V. Enforcement	448
VI. Distribution	448
<i>IT Management Policy</i>	<i>450</i>
I. Overview	450
II. Purpose	450
III. Scope	450

IV. Policy.....	450
A. RESPONSIBILITY TO MAINTAIN FUNCTIONALITY.....	451
B. SECURITY RESPONSIBILITIES	451
C. RESPONSIBILITY TO PREVENT UNAUTHORIZED OR INAPPROPRIATE ACCESS AND DISCLOSURE	453
D. PERMISSIBLE ACCESS BY IT COORDINATORS, TECHNICAL MANAGERS, AND STAFF	453
E. INVESTIGATION OF MISCONDUCT.....	453
F. WHERE REQUIRED BY LAW.....	454
G. ACCESS FOR COWORKERS	454
H. RESPONSIBILITY FOR POLICY ADHERENCE	454
I. SYSTEM USER RESPONSIBILITIES	454
J. MAINTENANCE OF INFORMATION SYSTEMS	455
V. Enforcement	455
VI. Distribution	455
<i>Logging Policy</i>	<i>457</i>
I. Overview	457
II. Purpose	457
III. Scope.....	457
IV. Policy.....	457
A. Underlying requirements.....	458
B. Activities to be logged	458
C. Elements of the log	459
D. Formatting and storage	460
E. Information Security Issues	461
V. Enforcement	462
VI. Distribution	462
<i>Logical Access Controls Policy</i>	<i>463</i>
I. Overview	463
II. Purpose	463
III. Scope.....	463
IV. Policy.....	463
V. Enforcement	465
VI. Distribution	465
<i>Mass Communication Policy</i>	<i>466</i>
I. Overview	466
II. Purpose	466
III. Scope.....	466
IV. Policy.....	466

V. Enforcement	467
VI. Distribution	467
<i>Mergers and Acquisitions Policy.....</i>	469
I. Overview	469
II. Purpose	469
III. Scope	469
IV. Policy.....	469
A. M&A Assessment Team	469
B. Security Requirements	470
C. M&A Assessment Report	470
V. Enforcement	470
VI. Distribution	470
<i>Mobile Device Policy.....</i>	472
I. Overview	472
II. Purpose	472
III. Scope	472
IV. Policy.....	472
V. Enforcement	474
VI. Distribution	474
<i>Network Address Policy</i>	476
I. Overview	476
II. Purpose	476
III. Scope	476
IV. Policy.....	476
V. Enforcement	477
VI. Distribution	477
<i>Network Configuration Policy</i>	479
I. Overview	479
II. Purpose	479
III. Scope	479
IV. Policy.....	479
V. Enforcement	482

VI. Distribution	482
Network Documentation Policy	484
I. Overview	484
II. Purpose	484
III. Scope	484
IV. Policy	484
V. Enforcement	485
VI. Distribution	485
Network Security Policy	487
I. Overview	487
II. Purpose	487
III. Scope	487
IV. Policy	487
A. Classification	487
B. Network Segmentation	489
C. Trusted Points	489
D. Security Controls	490
E. Data in Transit	493
F. Responsibilities	493
V. Enforcement	493
VI. Distribution	493
Outsourcing Policy	495
I. Overview	495
II. Purpose	495
III. Scope	495
IV. Policy	495
V. Enforcement	497
VI. Distribution	497
Password Policy	498
I. Overview	498
II. Purpose	498
III. Scope	498
IV. Policy	498
A. New User Accounts	499

B. Selecting Passwords/Phrases	499
C. Password/Phrase Guidelines.....	500
D. Password Changes	500
E. Software Applications	500
V. Enforcement	501
VI. Distribution	501
<i>Patch Management Policy</i>	<i>502</i>
I. Overview	502
II. Purpose	502
III. Scope.....	502
IV. Policy.....	502
V. Enforcement.....	503
VI. Distribution	503
<i>PCI Policy.....</i>	<i>504</i>
I. Overview	504
II. Purpose	504
III. Scope.....	504
IV. Policy.....	504
V. Enforcement.....	508
VI. Distribution	508
<i>Personnel Security Policy</i>	<i>510</i>
I. Overview	510
II. Purpose	510
III. Scope.....	510
IV. Policy.....	510
V. Enforcement.....	511
VI. Distribution	511
<i>Physical Access Policy</i>	<i>513</i>
I. Overview	513
II. Purpose	513
III. Scope.....	513
IV. Policy.....	513

V. Enforcement	516
VI. Distribution	516
<i>Physical Security Policy.....</i>	517
I. Overview	517
II. Purpose	517
III. Scope	517
IV. Policy.....	517
V. Enforcement	519
VI. Distribution	520
<i>Portable Computing Policy.....</i>	521
I. Overview	521
II. Purpose	521
III. Scope	521
IV. Policy.....	521
V. Enforcement	522
VI. Distribution	522
<i>Privacy Policy</i>	523
I. Overview	523
II. Purpose	523
III. Scope	523
IV. Policy.....	523
A. Individual Privacy Rights	523
B. Staff Privacy Rights.....	524
C. Privacy Controls	524
D. Security Controls.....	525
V. Enforcement	526
VI. Distribution	526
<i>Problem Management Policy.....</i>	527
I. Overview	527
II. Purpose	527
III. Scope	527
IV. Policy.....	527
A. Background	527

B. Preventive Controls.....	528
C. Detective Controls.....	529
D. Corrective Controls	530
E. Training.....	530
V. Enforcement	531
VI. Distribution	531
<i>Procedure Template</i>	<i>532</i>
I. Overview	532
II. Purpose	532
III. Scope.....	532
IV. Procedure.....	532
V. Enforcement.....	532
VI. Distribution	532
<i>Production Input Output Controls Policy</i>	<i>534</i>
I. Overview	534
II. Purpose	534
III. Scope.....	534
IV. Policy.....	534
V. Enforcement.....	535
VI. Distribution	535
<i>Quality Assurance Policy.....</i>	<i>536</i>
I. Overview	536
II. Purpose	536
III. Scope.....	536
IV. Policy.....	536
V. Enforcement.....	537
VI. Distribution	537
<i>Ransomware Policy</i>	<i>539</i>
I. Overview	539
II. Purpose	539
III. Scope.....	539
IV. Policy.....	539

V. Enforcement.....	540
VI. Distribution	540
<i>Remote Access Policy.....</i>	<i>541</i>
I. Overview	541
II. Purpose	541
III. Scope.....	541
IV. Policy.....	541
V. Enforcement.....	542
VI. Distribution	542
<i>Removable Media Policy.....</i>	<i>544</i>
I. Overview	544
II. Purpose	544
III. Scope.....	544
IV. Policy.....	544
V. Enforcement.....	546
VI. Distribution	546
<i>Reporting Violations Policy.....</i>	<i>547</i>
I. Overview	547
II. Purpose	547
III. Scope.....	547
IV. Policy.....	547
V. Enforcement.....	548
VI. Distribution	548
<i>Resilience Policy</i>	<i>549</i>
I. Overview	549
II. Purpose	549
III. Scope.....	549
<i>IV. Policy Working together, the MGMT and RMO shall:.....</i>	<i>549</i>
V. Enforcement.....	551
VI. Distribution	551
<i>Risk Assessment Policy</i>	<i>552</i>

I. Overview	552
II. Purpose	552
III. Scope	552
IV. Policy.....	552
A. Risk Assessments	552
B. Risk Analysis	553
C. Risk Treatment Plan	554
V. Enforcement	554
VI. Distribution	555
<i>Risk Management Policy</i>	<i>556</i>
I. Overview	556
II. Purpose	556
III. Scope	556
IV. Policy.....	556
A. Executive Management Reponsibilities	557
B. Risk Management Officer Responsibilities.....	557
C. Department Head Responsibilities.....	560
D. Chief Security Officer Responsibilities	562
V. Enforcement	562
VI. Distribution	562
<i>Router Security Policy.....</i>	<i>564</i>
I. Overview	564
II. Purpose	564
III. Scope	564
IV. Policy.....	564
V. Enforcement	565
VI. Distribution	565
<i>Secure Software Development Lifecycle Policy</i>	<i>567</i>
I. Overview	567
II. Purpose	567
III. Scope	567
IV. Policy.....	567
A. Software Development Lifecycle	567
B. Roles and Responsibilities	568
C. Secure Software Development Lifecycle Procedures	568

V. Enforcement.....	571
VI. Distribution	571
<i>Securing Information Systems Policy.....</i>	573
I. Overview	573
II. Purpose	573
III. Scope.....	573
IV. Policy.....	573
A. Information Systems Risk Management	574
B. Information System Life Cycle.....	574
C. Audit and Monitoring Techniques.....	575
D. General Information Systems Security Procedures	575
E. Incident Response Handling.....	579
F. Emergencies and Disasters.....	579
V. Enforcement.....	579
VI. Distribution	579
<i>Securing Sensitive Information Policy.....</i>	581
I. Overview	581
II. Purpose	581
III. Scope.....	581
IV. Policy.....	581
V. Enforcement.....	586
VI. Distribution	586
<i>Security Awareness and Training Plan</i>	587
I. Purpose of the Security Awareness and Training Plan.....	587
II. Overview of the Security Awareness and Training Plan.....	587
III. Security Awareness and Training Lifecycle.....	588
IV. Designing the Security Awareness and Training Program.....	589
V. Developing Material for the Security Awareness and Training Program	591
VI. Implementing a Security Awareness and Training Program	593
VII. Security Awareness and Training Program Post-Implementation	593
Appendix A – Distribution List	595
Appendix B – Receipt and Acknowledgement	595
<i>Security Awareness and Training Policy</i>	596

I. Overview	596										
II. Purpose	596										
III. Scope	596										
IV. Policy	596										
V. Enforcement	598										
VI. Distribution	598										
Security Controls Review Policy	600										
I. Overview	600										
II. Purpose	600										
III. Scope	600										
IV. Policy	600										
V. Enforcement	601										
VI. Distribution	601										
Security Monitoring Policy	603										
I. Overview	603										
II. Purpose	603										
III. Scope	603										
IV. Policy	603										
V. Enforcement	604										
VI. Distribution	605										
Security Policy	606										
<table border="1"> <tr> <td>Policy Area</td> <td>IT Policy Library</td> </tr> <tr> <td>Approved Date</td> <td>June 30, 2020</td> </tr> <tr> <td>Approved By</td> <td>Policy Committee</td> </tr> <tr> <td>Effective Date</td> <td>July 1, 2020</td> </tr> <tr> <td>Current Version</td> <td>2.1</td> </tr> </table>		Policy Area	IT Policy Library	Approved Date	June 30, 2020	Approved By	Policy Committee	Effective Date	July 1, 2020	Current Version	2.1
Policy Area	IT Policy Library										
Approved Date	June 30, 2020										
Approved By	Policy Committee										
Effective Date	July 1, 2020										
Current Version	2.1										
....	606										
I. Overview	606										
II. Purpose	606										
III. Scope	606										
IV. Policy	606										
A. Security Overview	606										
B. Administrative Safeguards	607										
C. Technical Safeguards	608										

D. Physical Safeguards.....	612										
V. Enforcement	613										
VI. Distribution	613										
<i>Security Self Assessment Policy</i>	<i>614</i>										
I. Overview	614										
II. Purpose	614										
III. Scope	614										
IV. Policy.....	614										
V. Enforcement	616										
VI. Distribution	616										
<i>Server Certificates Policy.....</i>	<i>617</i>										
I. Overview	617										
II. Purpose	617										
III. Scope	617										
IV. Policy.....	617										
V. Enforcement	618										
VI. Distribution	618										
<i>Server Hardening Policy.....</i>	<i>620</i>										
I. Overview	620										
II. Purpose	620										
III. Scope	620										
IV. Policy.....	620										
V. Enforcement	621										
VI. Distribution	621										
<i>Server Hardening Procedure</i>	<i>623</i>										
<table border="1"> <tr> <td>Policy Area</td> <td>IT Policy Library</td> </tr> <tr> <td>Approved Date</td> <td>June 30, 2020</td> </tr> <tr> <td>Approved By</td> <td>Policy Committee</td> </tr> <tr> <td>Effective Date</td> <td>July 1, 2020</td> </tr> <tr> <td>Current Version</td> <td>2.1</td> </tr> </table>	Policy Area	IT Policy Library	Approved Date	June 30, 2020	Approved By	Policy Committee	Effective Date	July 1, 2020	Current Version	2.1	
Policy Area	IT Policy Library										
Approved Date	June 30, 2020										
Approved By	Policy Committee										
Effective Date	July 1, 2020										
Current Version	2.1										
	 623										
I. Overview	623										
II. Purpose	623										

III. Scope.....	623
IV. Procedure.....	623
V. Enforcement.....	625
VI. Distribution	625
<i>Smartphone Policy.....</i>	627
I. Overview	627
II. Purpose	627
III. Scope.....	627
IV. Policy.....	627
V. Enforcement.....	628
VI. Distribution	628
<i>Social Networking Policy</i>	630
I. Overview	630
II. Purpose	630
III. Scope.....	630
IV. Policy.....	630
V. Enforcement.....	633
VI. Distribution	633
<i>Software Development Policy</i>	634
I. Overview	634
II. Purpose	634
III. Scope.....	634
IV. Policy.....	634
A. Software Development Life Cycle (SDLC).....	634
B. Access Controls	635
C. Data Owners	636
D. Quality assurance	636
E. Software Security	637
V. Enforcement.....	638
VI. Distribution	638
<i>Software Licensing Policy.....</i>	639
I. Overview	639
II. Purpose	639

III. Scope.....	639
IV. Policy.....	639
V. Enforcement.....	640
VI. Distribution	640
Staffing Policy	642
I. Overview	642
II. Purpose	642
III. Scope.....	642
IV. Policy.....	642
V. Enforcement.....	643
VI. Distribution	643
System and Organization Controls (SOC 2) Policy	645
I. Overview	645
II. Purpose	645
III. Scope.....	645
IV. Policy.....	645
V. Enforcement.....	646
VI. Distribution	646
System Security Plan.....	648
I. Purpose of the System Security Plan	648
II. Overview of the System Security Plan	648
III. Security Policy.....	648
IV. Risk Assessment.....	649
A. Assets	649
One of the first steps is to identify important assets. This includes facilities, network infrastructure components, customer data, intellectual property, etc. Without a complete and accurate inventory of IT assets, criticality and impact on the organization cannot be determined.....	649
B. Threats	649
C. Vulnerabilities	650
D. Impact.....	650
V. Risk Analysis	650
VI. Risk Response	651
Appendix A – Distribution List	652
Appendix B – Receipt and Acknowledgement	652

<i>System Update Policy</i>	<i>653</i>
I. Overview	653
II. Purpose	653
III. Scope.....	653
IV. Policy.....	653
A. Update Monitoring	653
B. Update Preparation	654
C. Applying Updates	654
V. Enforcement	655
VI. Distribution	655
TERMS AND DEFINITIONS POLICY	656
I. Overview	656
II. Purpose	656
III. Scope.....	656
IV. Policy.....	656
V. Enforcement	659
VI. Distribution	659
<i>Third Party Service Providers Policy</i>	<i>660</i>
I. Overview	660
II. Purpose	660
III. Scope.....	660
IV. Policy.....	660
V. Enforcement	664
VI. Distribution	664
<i>User Privilege Policy</i>	<i>666</i>
I. Overview	666
II. Purpose	666
III. Scope.....	666
IV. Policy.....	666
A. Types of users	666
B. Network resources	667
C. Security Considerations	668
V. Enforcement	668

VI. Distribution	668
<i>Vendor Access Policy</i>	<i>670</i>
I. Overview	670
II. Purpose	670
III. Scope	670
IV. Policy	670
V. Enforcement	672
VI. Distribution	672
<i>Virtual Private Network (VPN) Policy</i>	<i>674</i>
I. Overview	674
II. Purpose	674
III. Scope	674
IV. Policy	674
V. Enforcement	675
VI. Distribution	675
<i>Vulnerability and Penetration Testing Policy</i>	<i>677</i>
I. Overview	677
II. Purpose	677
III. Scope	677
IV. Policy	677
V. Enforcement	678
VI. Distribution	679
<i>Wearable Computing Device Policy</i>	<i>680</i>
I. Overview	680
II. Purpose	680
III. Scope	680
IV. Policy	680
V. Enforcement	681
VI. Distribution	681
<i>Web Site Policy</i>	<i>683</i>
I. Overview	683

II. Purpose	683
III. Scope	683
IV. Policy	683
V. Enforcement	684
VI. Distribution	685
Web Site Privacy Policy	686
I. Overview	686
II. Purpose	686
III. Scope	686
IV. Policy	686
A. Overview	686
B. Recommended Web Site Privacy Policy Content	687
V. Enforcement	691
VI. Distribution	691
Wireless Access Policy	693
I. Overview	693
II. Purpose	693
III. Scope	693
IV. Policy	693
A. Introduction	693
B. Connectivity Considerations	694
C. Security	694
V. Enforcement	695
VI. Distribution	695
Workstation Hardening Policy	697
I. Overview	697
II. Purpose	697
III. Scope	697
IV. Policy	697
V. Enforcement	698
VI. Distribution	698
Workstation Hardening Procedure	700
I. Overview	700

II. Purpose	700
III. Scope	700
IV. Procedure	700
V. Enforcement	701
VI. Distribution	702
<i>Workstation Security Policy</i>	<i>703</i>
I. Overview	703
II. Purpose	703
III. Scope	703
IV. Policy	703
V. Enforcement	704
VI. Distribution	705
<i>Receipt and Acknowledgement</i>	<i>706</i>

ACCEPTABLE USE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Information systems are a growing and important resource for F2OnSite Staff, one that can provide critical competitive advantage to F2OnSite in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our Staff use Information Systems to connect with our customers, suppliers and other key organizations, it is important that F2OnSite Staff understand and agree on the appropriate procedures to protect F2OnSite's assets.

II. Purpose

This policy provides useful tips and techniques to promote effective use of F2OnSite's Information Systems. It applies to all F2OnSite systems located on or accessed from F2OnSite property and systems provided by F2OnSite for use in F2OnSite business.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

F2OnSite utilizes sophisticated computer and communications systems to assist Staff in performing their job functions. These technologies support our business activities by enabling closer, more effective and timely communications among personnel within the F2OnSite and with our customers, partners and vendors worldwide. These guidelines advise all users regarding the access to and the disclosure of Information Systems. These guidelines establish the F2OnSite's expectations for all Staff concerning the disclosure of information via F2OnSite's Information Systems.

F2OnSite maintains and uses many facilities, equipment, and communication systems, such as telephones, regular mail, special delivery services, E-mail, voice mail, fax machines, computers, etc., designed to make the F2OnSite's operations effective and efficient. F2OnSite's Information Systems are provided to Staff at F2OnSite expense to assist Staff in carrying out F2OnSite business. Some of these systems permit Staff to

communicate with each other internally and with other parties externally. As with all F2OnSite assets, F2OnSite's Information Systems are for official F2OnSite business only. Access to F2OnSite Information Systems is provided in conjunction with the official F2OnSite business and individual job responsibilities. Use of F2OnSite's Information Systems is subject to these policies and guidelines and other relevant F2OnSite policies and procedures.

A. INFORMATION ACCESS, CONTENT, AND USE

The F2OnSite makes every effort to provide its Staff with the best technology available to conduct the F2OnSite's official business. The F2OnSite has installed, at substantial expense, Information Resources to conduct its official business.

This document addresses general Information Systems policies and guidelines, specific issues related to appropriate content, and Staff use of F2OnSite's Information Systems. All departments and Staff are required to follow these general policies and guidelines. All F2OnSite Staff with access to F2OnSite's Information Systems are required to read, understand and comply with F2OnSite's policies.

F2OnSite's Information Systems are owned by F2OnSite and are to be used for business purposes only in serving the interests of F2OnSite's customers and in the course of normal business operations.

The use of F2OnSite facilities, property, equipment, or communication systems is limited to Acceptable Use as defined in these policies and guidelines. No F2OnSite equipment or communications systems, including all hardware and software, may be removed from F2OnSite property without prior express consent of the F2OnSite.

Personal equipment, including all computer hardware and software, may not be brought onto F2OnSite premises or be used for F2OnSite's official business without the prior express consent of the F2OnSite. Staff are not to use their personal accounts during work hours or use F2OnSite equipment to reach personal sites unless it is for legitimate business purposes, as determined solely by F2OnSite.

The F2OnSite encourages the use of F2OnSite's Information Systems for business when such business can be accomplished consistent with the following policies and guidelines identified in this document. When using Information Systems, Staff shall conduct official F2OnSite business consistent with the F2OnSite's mission statement. Official F2OnSite business shall comply with all federal and state statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official F2OnSite business conducted via the Internet should meet or exceed the standards of performance for traditional methods (e.g. meetings, use of telephone).

Staff shall base decisions to use F2OnSite's Information Systems on sound business practices. The conduct of business using F2OnSite's Information Systems is

particularly compelling where costs are reduced and/or the services provided by the F2OnSite are improved in measurable ways. When using F2OnSite's Information Systems, F2OnSite Staff shall promote and maintain a professional image.

F2OnSite Staff shall disseminate information that is current, accurate, complete, and consistent with F2OnSite policy. Information released via F2OnSite's Information Systems is subject to the same official F2OnSite policies for the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important.

F2OnSite Staff shall protect confidential and proprietary information entrusted to the F2OnSite. Questions regarding confidential or proprietary information should be directed to F2OnSite management or his/her designee.

B. PROTECTING CONFIDENTIAL INFORMATION

Maintaining the confidentiality of sensitive information is crucial to F2OnSite's success. Confidential information stored on or carried over F2OnSite's Information Systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review unless Staff take the necessary precautions outlined in these guidelines.

F2OnSite has developed specific procedures to ensure the protection of confidential information. Staff should exercise care when communicating any potentially confidential information outside of F2OnSite, as no electronic communications facility is completely secure.

Data shall be classified per the Data Classification Policy. All confidential data should be marked with "Confidential," "Do not reproduce," "Not to be reproduced without approval," or "Do not forward." All E-mail messages containing confidential information should contain "Confidential" in the subject header.

Some directories in the F2OnSite's Information Systems contain sensitive or confidential data. Access to these directories shall be restricted. Unauthorized attempts to circumvent such access restrictions are violations of these Guidelines and may result in disciplinary action, up to and including termination of employment, and legal action.

Staff must refrain from entering into discussions with third parties regarding the F2OnSite's business prospects or financial condition. Staff should not discuss future products, services, features or functionality unless F2OnSite has previously disclosed such information in a press release or through some other public disclosure. Such information is proprietary to F2OnSite and constitutes valuable information that should be protected as a trade secret. The release of such information could become the subject of criminal prosecution.

Staff are asked to respect the privacy of individuals who send them messages. Staff should protect voice mail, and E-mail accounts from unauthorized access. Appropriate protection procedures include ensuring proper password protection to these accounts, closing E-mail messages after reading them and deleting all messages when they are no longer needed.

Staff shall not place F2OnSite material (e.g. copyrighted software, internal correspondence) on any publicly accessible Internet computer without prior permission.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Staff must exercise caution and care when transferring such material in any form.

C. COPYRIGHTED INFORMATION

F2OnSite respects the intellectual property rights of other companies and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. F2OnSite's Information Systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Staff should not assume that merely because information is available on an electronic information system such as the Internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, F2OnSite management should be consulted.

All material trademarked or copyrighted by F2OnSite should be marked with the appropriate trademark or copyright designation. No F2OnSite Staff should remove trademark and copyright notices from third party material.

F2OnSite's license to use software is carefully set forth in legal agreements that F2OnSite has with the developers and distributors of the software. Staff's use of software must be in compliance with those agreements. If F2OnSite gives Staff the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless Staff are given prior express consent by F2OnSite management. When Staff leave F2OnSite, all F2OnSite owned software, licenses, and media will remain with F2OnSite.

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, Staff members are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

D. PRIVACY STATEMENT

This policy is intended to guide Staff in the performance of their duties. It is also intended to place Staff on notice that Staff should not expect F2OnSite's Information Systems and their contents, to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No Staff member has a reasonable expectation of personal privacy with respect to the use of any of the F2OnSite's facilities, property, equipment or communications systems. This includes anything created or received on F2OnSite's Information Systems even if used for business purposes and in the normal course of F2OnSite operations.

F2OnSite reserves the right, but not the obligation, to monitor use of F2OnSite's Information Systems including the Internet, E-mail, computer transmissions, and electronically stored information created or received by F2OnSite Staff with the F2OnSite's Information Systems. All computer applications, programs, work-related information created or stored by Staff on F2OnSite's Information Systems, are F2OnSite property.

E. MONITORING AND INSPECTING INFORMATION SYSTEMS

F2OnSite's Information Systems are provided for official F2OnSite business. F2OnSite's Information Systems are owned and controlled by the F2OnSite and are accessible at all times by the F2OnSite for maintenance, upgrades and other business or legal purposes.

All Information Systems, including the messages and data stored on the systems, are and remain at all times the property of F2OnSite, subject to applicable third party intellectual property rights such as copyrights. By virtue of continued employment and use of F2OnSite systems, all Staff are considered to have consented to monitoring and other access by authorized F2OnSite personnel. F2OnSite reserves the right to inspect a Staff member's computer system for violations of F2OnSite policies.

F2OnSite reserves the right to access and conduct an inspection or search all directories, indices, files, databases, faxes, F2OnSite computer hardware and software, voice mail, E-mail and communication systems or deliveries sent to any F2OnSite location, and other Information Resources no matter to whom it is addressed, with no prior notice. F2OnSite may also cancel or restrict any Staff's privilege to use any or all of its facilities, equipment, property, or communication systems.

If a Staff member refuses to cooperate with a search or inspection for legitimate business purposes that is based on reasonable suspicion that the Staff is in possession of prohibited materials, F2OnSite may take that refusal into consideration in determining appropriate disciplinary action. A Staff member's refusal to provide their password to F2OnSite management will be considered additional grounds for discipline. Discipline,

including termination, will be based on all available information, including the information giving rise to the inspection or search.

Access to on-line services, the Internet, blogs, social media sites, or other communications networks is prohibited unless F2OnSite has provided prior express consent. As such, no F2OnSite equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Employee use of these services may be monitored to include numbers called and the amount of time spent using the services. F2OnSite reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

F2OnSite management may examine Staff communications or files and such examination should be expected to occur in various circumstances when necessary, including, but not limited to:

- Ensuring that F2OnSite systems are not being used to transmit discriminatory, harassing or offensive messages of any kind.
- Determining the presence of illegal material or unlicensed software.
- Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
- Investigating allegations or indications of impropriety.
- Locating, accessing and/or retrieving information in Staff absence.
- Responding to legal proceedings and court orders in the preservation or production of evidence.
- F2OnSite reserves the right to review Staff use of and to inspect all material created by or stored on F2OnSite Information Systems. F2OnSite reserves the right to monitor all use of Information Systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of F2OnSite, subject to access, review, duplication, deletion, or disclosure by F2OnSite management or by other personnel authorized by F2OnSite. Staff should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to the F2OnSite. Staff should treat F2OnSite's Information Systems with the expectation that communications will be available for review by authorized personnel of F2OnSite for legitimate business purposes at any time.

F2OnSite reserves the right to access, review, duplicate, delete or disclose for legitimate business purposes any communications, messages or data derived from use of F2OnSite's Information Systems.

F. STORING AND ARCHIVING INFORMATION

F2OnSite has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By virtue of various archival practices employed at F2OnSite, any messages or data stored, even temporarily, on F2OnSite Information Systems may be copied to magnetic or other storage media without the specific knowledge of the individual creating the messages or data. Such archives are and remain F2OnSite property and may be used by the F2OnSite for any business purpose. Simply deleting messages or data from these Information Systems does not provide privacy with regard to such messages or data. The length of time that such archives may be maintained can be almost indefinite. Staff may be required to preserve their electronic data based on pending litigation and/or investigations by the F2OnSite. Refer to the Data Retention Policy for more information on storing and archiving information.

G. EMPLOYEE USAGE

Each Staff has the responsibility of complying with F2OnSite's policies and guidelines provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

The use of Information Systems is restricted to official F2OnSite business. Personal use of or time spent for personal gain is strictly prohibited unless F2OnSite gives prior express consent. Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any Internet use that could cause congestion, disruption of normal service, or general additional F2OnSite expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Staff should be aware that F2OnSite's Information Systems and the World Wide Web are not censored and contain information some users may find offensive. F2OnSite cannot accept responsibility for what the Staff accesses. However, if offensive material is accessed, Staff shall disengage from the material immediately.

Staff shall not copy or transfer electronic files without prior F2OnSite permission. Almost all software is subject to Federal copyright laws. Care should be exercised

whenever accessing or copying any information that does not belong to the Staff. When in doubt, consult F2OnSite management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on F2OnSite's Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the Internet can infect F2OnSite's systems with a virus. Staff shall not circumvent or disable F2OnSite standard virus prevention software and/or Information Resource security mechanisms.

Staff shall not send post or provide access to any confidential F2OnSite materials or information to anyone outside of F2OnSite.

Staff are obligated to cooperate with any investigation regarding the use of Staff computer equipment and which F2OnSite management has authorized.

Alternate Internet Service Provider connections to F2OnSite's internal network are not permitted unless prior express consent has been given by F2OnSite management and properly protected by a firewall or other appropriate security device(s).

If Staff are using information from an Internet site for strategic official F2OnSite business decisions, Staff should verify the integrity of that information. Staff should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information.

F2OnSite has no control or responsibility for content on an external server not under the control of the F2OnSite. Information may be offensive and/or unsuitable for dissemination.

Do not upload or download large files during prime hours due to the network impact on other users. Information Systems may have limits regarding disk space usage. Documents take up space; therefore, Staff should regularly delete and/or archive any files Staff wish to save.

Staff using F2OnSite's accounts are acting as representatives of the F2OnSite. As such, Staff should act accordingly so as not to damage the reputation of F2OnSite.

H. INFORMATION SYSTEMS AWARENESS

The use of Information Systems is the responsibility of each Staff. The practices listed below are not inclusive, but rather designed to remind each Staff of the need to raise their Information Systems awareness.

- Protect equipment. Keep it in a secure environment and keep food and drink from electronic systems. Know where the fire suppression equipment is located and how to use it in an emergency.
- Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area
- Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the Staff. Change the password often and change it immediately if it has been compromised.
- Protect files. Don't allow unauthorized access to Staff files and data. Never leave equipment unattended with the password activated – log off.
- Backing up data. Keep duplicates of critical data in a safe place.
- Report security violations. Staff should tell their supervisor or F2OnSite management if Staff see any unauthorized changes to Staff data. Immediately report any loss of data or programs, whether automated or hard copy.

I. ELECTRONIC MAIL (E-MAIL) AND ETIQUETTE

E-mail may be sent through each Staff's computer. E-mail will be sent for official F2OnSite business only. No personal E-mail shall be sent or received via F2OnSite Internet accounts.

F2OnSite Staff should not attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. Management reserves the right, but not the obligation, to access all E-mail files created, received or stored on F2OnSite-funded systems and such files can be accessed without prior notification.

F2OnSite Staff are expected to maintain their E-mail accounts on a regular basis. This entails deleting E-mail once it has been read or sent. Excess E-mail takes up unnecessary storage space on the server and may cause the entire system to run slowly.

E-mail requires extensive network capacity. Sending unnecessary E-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical official F2OnSite business. When F2OnSite grants an individual Staff access to the network, it is the responsibility of Staff to be cognizant and respectful of network resources.

E-mail users are to exercise good judgment and common sense when creating and distributing messages. E-mail is the property of the F2OnSite and is to be used exclusively for official F2OnSite business. No Staff E-mail is considered private. Similarly, the accessing, reading or copying of E-mail not intended for a Staff member's eyes is prohibited. Staff are strictly prohibited from sending E-mail messages of a

harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Staff are prohibited from using aliases while connected to services. F2OnSite retains the right to access a Staff member's E-mail at any time for any reason without notice to the Staff. Conduct in violation of this policy will subject an Staff to F2OnSite's disciplinary procedures.

Mail on the internet is not secure. Never include in an E-mail message anything private and confidential. E-mail is sent unencrypted and is easily read. If anything but plain text is sent as an E-mail, be careful. Recipients may not have the ability to translate other documents, for example Word or Excel documents.

State the subject of the message in the subject line.

Include a signature (an identifier that automatically appends to the E-mail message) that contains the method(s) by which others can contact Staff (usually Staff's E-mail address, phone number, faxes number, etc.).

For important items, let senders know Staff has received their E-mail, even if Staff cannot respond in depth immediately. They need to know their E-mail is not lost.

Watch punctuation and spelling. It can reflect on Staff's professionalism. Use automatic spell checking programs if available.

Be careful when sending replies - make sure Staff is sending to a group when intent is to send to a group and to an individual when Staff intent is to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.

Never send angry messages (flames). If an Staff receives a "flame", do not over react. Remember that not everyone is polite. **DO NOT SEND MESSAGES ALL IN CAPITALS.** It looks like shouting. Use initial capitals or some other symbol for emphasis. For example: That **IS** what I meant. That **is** what I meant.

Remember that some people have to pay for each byte of data they receive. Please keep messages to the point without appearing terse or rude.

The use of Information Systems should be consistent with F2OnSite's core values when communicating with both Staff and external parties. Particularly, the values of honesty, integrity and mutual respect should govern Staff's use of Information Systems. When using voice mail and E-mail systems for communicating with other individuals over Information Systems, Staff should consider the following principles:

- Be courteous - Refrain from saying anything electronically that you would not say to the recipient face-to-face.

- Keep messages brief - Include only one topic per message, and start the main point in the first sentence.
- Proofread messages - E-mail messages drafted in haste can be difficult to follow and easy to misinterpret. Do not ignore the basics of writing in E-mail correspondence.
- Use a descriptive subject line - When using E-mail, never leave a subject line blank. Remember to use brief but informative message headers.
- Properly prioritize - Do not overstate the urgency of the message simply to get attention. "Urgent" designations should be limited to messages that require immediate response from the recipient.
- Send messages only to appropriate individuals - Send E-mail on a need-to-know basis only. Unnecessary messaging should be avoided as it decreases the effectiveness of F2OnSite systems.
- Identify the message sender - No E-mail or other electronic communication may be sent which attempts to hide the identity of the sender, or represent the sender as someone else or from another organization.
- Use attachments wisely - Some individuals have systems that cannot read attachments in E-mail messages. Staff using UNIX workstations may not be able to read attached Word documents. Voice mail attachments may contain irrelevant information.
- Respond with care - Be careful not to use "Reply all" unless you intend all other recipients to receive your response.
- Think before forwarding messages - Think of the sender's intentions before forwarding private communications.

J. SECURING INFORMATION SYSTEMS WITH PASSWORDS

Prior express consent for Information Systems access must be obtained through F2OnSite management. Staff of contractors shall only be given access to the network after written communication and approval by F2OnSite management. Once F2OnSite provides prior express consent, Staff shall be responsible for the security of their account password and will be held responsible for all use or misuse of his or her account. No other password or security device shall be used without approval by F2OnSite management.

Each F2OnSite Information System may allow Staff to set or change their password. If so, set the password and change it regularly. Guidelines for choosing and setting passwords should be obtained from the Password Policy. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user. After logging on, the computer will attribute all activity to a Staff member's user id. Therefore, never leave workstations without logging off -- even for a few minutes.

Always log off or otherwise inactivate the workstation so no one could perform any activity under Staff's user id when away from the area. Staff should safeguard sensitive information from disclosure to others.

If requested, Staff shall disclose their passwords (e.g. voice mail, E-mail, relevant Internet web site passwords) to their supervisor and/or manager. Staff must maintain secure passwords and never use an account assigned to another user.

F2OnSite reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when Staff leaves the F2OnSite, or at any other appropriate time, the F2OnSite may replace Staff's password with another of the F2OnSite's choosing.

K. PROTECTING INFORMATION SYSTEMS

F2OnSite provides virus protection software to help safeguard Information Systems. These systems are not totally foolproof. As such, be particularly cautious when opening any E-mail with an attachment.

Staff shall not disable or remove anti-virus software. Viruses can infect executable files, disk boot sectors, documents, etc. If a virus is received from a sender, that sender should be notified that the file was infected and, if possible, the type of virus should be identified.

Network administrators shall ensure that only fully supported web browsers and e-mail clients are allowed to execute in the organization, ideally only using the latest version of the browsers and e-mail clients provided by the vendor.

Network administrators shall use Domain Name System (DNS) filtering services to help block access to known malicious domains. To lower the chance of spoofed or modified e-mails from valid domains, network administrators shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

L. ENCRYPTING DATA

Only authorized encryption tools (both software and hardware) may be used in connection with Information Systems. Except with the prior written consent of F2OnSite management, all encryption tools must permit the F2OnSite to access and recover all encrypted information.

M. SECURING MOBILE COMPUTING DEVICES

Staff who use F2OnSite mobile computing resources (laptops, hand held devices, etc.) must take adequate precautions to ensure that proprietary information contained in such

devices is secure and not available to third parties, particularly during travel. Staff are responsible for taking adequate precautions against theft of their mobile computing devices. Please refer to the Bring Your Own Device and Technology Policy for more information.

N. ACCEPTABLE USE

- **Authorized Use.** The authorized use of F2OnSite systems is limited to F2OnSite's official business. The F2OnSite provides Information Systems and communication tools to facilitate business communication and enhance personal productivity. F2OnSite reserves the right to prohibit or restrict use of F2OnSite systems for any other purpose and at any time.
- **Incidental Personal Use.** Personal use of F2OnSite systems is permitted so long as it is not excessive as determined by the F2OnSite, does not interfere with job performance, consume significant resources, or interfere with the activities of other Staff.

O. UNACCEPTABLE USE

- **Unauthorized Use.** Excessive personal and other use of Information Systems inconsistent with this or any other F2OnSite policy is unauthorized. Under no circumstances are F2OnSite's Information Systems to be used for personal financial gain or to solicit others for activities unrelated to official F2OnSite business, such as solicitations for personal, political, or religious causes. Installation of software without approval from F2OnSite management is unauthorized.
- **Disruptive Use.** Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous, harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or "broad band" distribution of E-mail would clearly constitute a disruptive use.
- **Prohibited use.** Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Information Systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, Staff should contact F2OnSite management. Staff are

expressly prohibited from using F2OnSite's Information Systems to store or access pornography.

Only the IT Department is authorized to install software on servers, storage, and other related Information Resources.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who use Information Resources.

Policy History

Version	Date	Description	Approved By
2.0	6/30/2020	Initial policy release	D. Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT APO01.02, APO01.11, APO07.03, APO07.05, APO13.01, APO13.02, DSS04.05
GDPR Article 32
HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)
ISO 27001 7.3, A.7.2, A.8.1.3, A.8.2
NIST SP 800-37 3.3
NIST SP 800-53 3.2, 3.4, 3.16
NIST Cybersecurity Framework ID.AM-6, ID.GV-2, DE.DP-2
PCI 12.3.5

ACCESS CONTROL POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite's Information Systems are provided as a central resource for F2OnSite Staff. It is important that the network infrastructure, which includes cabling and associated devices continues to develop with sufficient flexibility to meet F2OnSite demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

II. Purpose

The purpose of this policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of F2OnSite information.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

Users are permitted to access and use only approved Information Resources. Users inside the F2OnSite firewall may not connect to the F2OnSite network if they are using a wireless connection to connect to an external network.

Non-IT Staff shall not:

- Extend or re-transmit network services by installing a router, switch, hub, or wireless access point to the F2OnSite network
- Install network hardware or software that provides network services

- Alter network hardware in any way
- Download, install, or run security programs or utilities that reveal weaknesses in the security of a system
- Run password cracking programs, packet sniffers, network mapping tools, or port scanners

The Chief Security Officer shall ensure:

- The organization has implemented procedures for the authorization and/or supervision of employees who work with Sensitive Information or in locations where it might be accessed.
- Detailed job descriptions determine the appropriate level of access to Sensitive Information.
- Access to Information Systems is limited to authorized users and processes. Access to Information Systems is limited to the types of transactions and functions that authorized users are permitted to access. Users, processes, and devices are authenticated before allowing access to Information Systems. Controls shall be implemented and maintained to ensure Information System users, and processes acting on behalf of users or devices, are properly identified.
- A process exists to establish and maintain access to Sensitive Information. Similar processes exist to control access to paper records.
- Procedures exist to ensure the access of an employee to Sensitive Information is appropriate and the procedures are used consistently.
- Procedures protect Sensitive Information from parent organizations and subsidiaries. Technical safeguards exist to separate Sensitive Information used by F2OnSite to protect against unauthorized access by other organizations.
- Procedures grant access to Sensitive Information through access to a workstation, device, transaction, program, or process. Procedures specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of a specific device that can access Sensitive Information.
- Procedures identify devices that access Sensitive Information and those that do not. Procedures specify where to place and position workstations to only allow viewing by authorized individuals. Procedures specify the use of additional security measures (e.g. privacy screens, password protected screen savers, auto logoff, etc.) to protect workstations with Sensitive Information.
- Procedures address device use for users that access Sensitive Information from remote locations.
- Procedures specify that electronic sessions be terminated after a specified period of inactivity. Automatic logoff is implemented on all devices that have access to

Sensitive Information. Refer to the Securing Information Systems Policy for more information.

- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
- Controls are implemented and maintained on connections to external Information Systems. Controls are implemented on information that is posted or processed on publically accessible Information Systems. Processes are implemented to ensure controls are sufficient and effective.
- Passwords/phrases are changed on a regular basis according to a schedule identified in the Password Policy.

Physical safeguards shall ensure only authorized Staff have access to Information Systems, equipment, and operating environments. For more information see:

- Facility Security Plan
- Physical Access Policy
- Physical Security Policy
-

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D.LAUDERBACK

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)
ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC1-7, DE.CM-1-3, DE.DP-2, RS.RP-1

PCI 7.1-3, PCI Software Security Framework

ACCOUNT MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Computer accounts are the means used to grant access to F2OnSite Information Resources. These accounts provide a means of providing accountability, a key to any computer security program, for information resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

II. Purpose

This policy establishes the rules for creating, monitoring, controlling, and removal of accounts.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

The Chief Security Officer shall ensure:

- System components and data resources that each role needs to access for their job function including level of privilege required (e.g. user, administrator, etc.) for accessing such resources.
- Security mechanisms restrict access to privileged user IDs to least privileges necessary to perform job responsibilities and such access is based on job classification and function.
- Documented approval by authorized parties specifying required privileges.
- Access control systems for systems components with multiple users that restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed.

This access control system must include the following: coverage of all system components, assignment of privileges to individuals based on job classification and function, and default “deny-all” setting.

- The organization has implemented procedures for terminating access to sensitive information when a Staff member leaves or has a change in job duties.
- Procedures assign responsibility for removing IT and/or physical access. Procedures include timely communication of termination actions to ensure that the procedures are appropriately followed.
- Procedures are based upon initial access authorization and subsequent modification of a user’s right of access to a workstation, transaction, program, or process.
- Procedures are in place for establishing and modifying user access to sensitive information. Such procedures shall be formally documented and updated regularly.
- Every 90 days a review of the list of persons with access to sensitive information shall be performed to ensure they are valid. Any inactive user accounts shall be immediately removed or disabled.
- The organization assigns a unique name and/or number for identifying and tracking user and administration identity. Procedures require the user ID to be in a specific format and specify the format to be used. Procedures specify that the unique user ID be used to track user activity within information systems that contain sensitive information. In addition to assigning a unique ID, IT security
- Staff shall employ at least one of the following methods to authenticate all users: something known (e.g. password or passphrase), something they have (e.g. token device or smart card), something they are (e.g. biometric). Where other authentication mechanisms are used (e.g. physical or logical security tokens, smart cards, certificates, etc.), authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. In addition, physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
- Shared user IDs shall not exist for system administration and other critical functions. Shared and generic user IDs are not to be used to administer Information Systems and components.
- Authentication procedures verify a person or entity seeking access to sensitive information is the one claimed. Policies specify the types of approved authentication mechanisms that are reasonable and appropriate and control the addition, deletion, and modification of User IDs, credentials, and other identifier objects.

- Configuration standards are developed for all system components. Such standards shall address all known security vulnerabilities and be consistent with industry accepted system hardening standards such as those recommended by the Center for Internet Security (CIS), International Standards Organization (ISO), SysAdmin Audit Network Security (SANS), and National Institute of Standards Technology (NIST).
- Security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
- An analysis of risks to determine when two-factor (multi-factor) authentication shall be implemented on user accounts and systems whether managed onsite or by a third-party provider. Two-factor authentication shall be required for remote network access originating from outside the network by personnel (including users and administrators) and all third-parties (including vendor access for support or maintenance). Note: Two-factor authentication requires two of the three authentication methods (i.e. something known, have, or biometric) be used to gain access to a system. Using two separate passwords is not considered two-factor authentication.

All accounts created must have an associated request and approval that is appropriate for the F2OnSite system or service.

All users must sign the F2OnSite non-disclosure agreement before access is given to an account. All accounts must be uniquely identifiable using the assigned user name.

IT security Staff shall:

- Always change all vendor supplied defaults and remove or disable unnecessary default or generic accounts before installing a system on the network. This includes firewalls, routers, servers, storage devices, wireless devices, etc. that are connected to sensitive data or used to transmit sensitive data.
- Ensure all default passwords are changed including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).
- Change wireless vendor defaults for environments containing or transmitting sensitive data. This includes, but is not limited to, default wireless encryption keys, passwords, and SNMP community strings.

- Ensure all default passwords for accounts must be constructed in accordance with the F2OnSite Password Policy. All accounts must have a password expiration that complies with the F2OnSite Password Policy.

Accounts of individuals on extended leave (more than 30 days) will be disabled. All new user accounts that have not been accessed within 30 days of creation will be disabled. Any accounts that cannot be associated with a business process or business owner shall be disabled.

System Administrators or other designated staff:

- Are responsible for removing the accounts of individuals that change roles within F2OnSite or are separated from their relationship with F2OnSite.
- Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
- Must have a documented process for periodically reviewing existing accounts for validity
- Are subject to independent audit review.
- Must provide a list of accounts for the systems they administer when requested by authorized F2OnSite management.
- Must cooperate with authorized F2OnSite management investigating security incidents.
- Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. For example, web servers, database servers, and DNS should be implemented on separate servers. Where virtualization technologies are in use, implement only one primary function per virtual system component.
- Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
- Configure system security parameters to prevent misuse.
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access management and other non-console administrative access.

- Maintain an inventory of Information Systems and related components.
- Verify user identity before modifying any authentication credential. For example, performing password resets, provisioning new tokens, or generating new keys.

Users of Information Systems shall be notified:

- Prior to gaining access to a system where system usage is monitored, recorded, and subject to audit.
- By using the system, he/she has granted consent to such monitoring and recording.
- Unauthorized use is prohibited and subject to criminal and civil penalties.
- If the operating system permits, each initial screen (displayed before user logon) shall contain warning text to the user and the user shall be required to take positive action to remove the notice from the screen.

Security personnel must ensure effective administration of users' computer access to maintain system security, including user account management, auditing, and the timely modification or removal of access. The following are important user administration considerations:

- User account management – Staff shall have a process for requesting, establishing, issuing, and closing user accounts. In addition, Staff should track users and their respective access authorizations.
- Audit and management reviews – on an annual basis, security personnel shall review system user accounts. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege (access to system components and data to only those individuals whose job requires such access), whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, etc. These reviews must be conducted on an application-by-application and on a system wide basis.
- Detecting unauthorized/illegal activities. Mechanisms besides auditing and analysis of audit trails must be used to detect unauthorized and illegal acts. Rotating Staff in sensitive positions, which could expose a scam that required a Staff member's presence, and periodic rescreening of personnel help manage risks.

Termination of a Staff member may be classified as either friendly or unfriendly. Friendly terminations must be accomplished by implementing a standard set of procedures for outgoing or transferring Staff. This normally includes:

- Removal of access privileges, computer accounts, authentication tokens.
- The control of keys to the office and/or office furniture and equipment.

- The briefing on the continuing responsibilities for confidentiality and privacy.
- Return of F2OnSite property.
- Replacement staff ability to access data.

Information security responsibilities and duties that remain valid after termination or change shall be defined, communicated to the appropriate Staff, and enforced.

F2OnSite requires terminating Staff to document procedures or filing schemes (e.g. how and where documents are stored on the hard disk). Staff must be instructed whether or not to "clean up" their computer before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.

Unfriendly Terminations have a potential for adverse consequences. In addition to the above, Staff shall do the following:

- System access must be terminated as quickly as possible when a Staff member is leaving a position under less than friendly terms. If Staff are to be immediately terminated, system access must be removed at the same time (or just before) Staff is notified of the dismissal.
- When a Staff member notifies F2OnSite of a resignation, and it can be reasonably expected that it is on unfriendly terms, system access must be immediately terminated.
- During the "notice of termination" period, it may be necessary to assign the individual to a restricted area and function. This may be particularly true for Staff capable of changing programs or modifying the system or applications.
- In some cases, physical removal of the Staff member from F2OnSite's offices may be necessary.
- Upon termination, Staff returns any items or assets that belong to F2OnSite.
- Upon change in Staff duties, the Owner of an asset shall determine the appropriate change in Staff access rights to Information Resources.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who use Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	7/1/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO01.01-03, APO01.11, APO12.02, APO12.07, APO13.01-02, APO13.07, DSS01.05

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC, DE.DP-2, RS.RP-1

PCI 7.1-3, 8.1-2

ACQUISITION AND PROCUREMENT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to protecting its employees, customers, partners, and its operations. This policy enables F2OnSite to effectively deliver equipment and services that meet the needs of the organization through innovative policy, guidance, and oversight. This policy is an effective way to direct F2OnSite's effort in procuring products and services.

II. Purpose

By incorporating environmental considerations in purchasing, F2OnSite can reduce its burden on the local and global environment, removing unnecessary hazards from its operations, reducing costs and liabilities, and potentially improving the environmental quality of the region.

This policy is intended to ensure that acquisitions support and enhance the capabilities of F2OnSite, provide F2OnSite with a competitive edge, and provide a standardized method of procuring products and services.

III. Scope

This policy applies to the Purchasing Department, IT Department, and senior executives.

IV. Policy

Where possible, acquisitions of products and services should be based upon clear and performance based requirements. The Purchasing Department shall ensure that the expected cost, delivery schedule, and performance outcomes are identifiable and measurable.

Benefits

- Acquisitions of services are properly planned and administered to achieve outcomes consistent with F2OnSite's needs.
- Products and services are acquired by business arrangements with are in the best interests of F2OnSite and are in compliance with applicable statutes, regulations, policies, and other requirements.
- Products and services are acquired using a strategic, enterprise-wide approach, which is applied to both the planning and execution of the acquisition.

The F2OnSite Purchasing Department Staff shall:

- Raise staff awareness on security and environmental issues affecting procurement by providing relevant information.
- Encourage suppliers and contractors to offer secure and environmentally preferable products and services at competitive prices.
- Encourage providers of products and services to consider security and the environmental impacts.
- Comply with all legislative and regulatory requirements in the procurement of products and services.

Where possible, F2OnSite should procure environmentally preferable products and services where criteria have been established by recognized authorities (e.g. Energy Star, EPA Eco Purchasing Guidelines, etc.). Staff should integrate environmental factors into buying decisions where external authorities have not established criteria.

Examples include:

- Replacing disposables with reusables or recyclables
- Supporting eco-labelling practices by buying products bearing such labels in preference to others, where they are available and provide value for money.
- Taking into account life cycle costs and benefits.
- Evaluating, as appropriate, the environmental performance of vendors in providing products and services.

F2OnSite's executive management retain the ability to respond rapidly to emergencies. Implementation of this policy is not intended to impede the timely acquisition of products and services in emergency situations.

A. PROCUREMENT ACTION

F2OnSite's Director of Purchasing shall be responsible for the management of acquisitions of products and services by or on behalf of F2OnSite's departments and staff. The Purchasing Department must:

- Comply with the requirements contained in this policy.

- Assign specific persons to review and approve the acquisition of products and services for each department.
- Ensure that acquisitions comply with applicable statutes, regulations, policies, and other requirements.
- Develop procedures for proposed acquisitions of products and services with estimated values exceeding notification thresholds.
- Ensure that the acquisition of products and services uses competition and performance based acquisitions to the maximum extent practicable.
- Ensure the collection of data on the acquisition of products and services for their area of responsibility.
- Monitor, require data collection, and conduct periodic acquisition and analysis of spending.

If a proposed acquisition includes both hardware and services, and the estimated total amount exceeds the notification thresholds, the acquisition must be approved by the appropriate F2OnSite Vice President.

F2OnSite executive management may identify any acquisitions as a special interest subject to review.

Consistent with F2OnSite's strategic sourcing initiative, executive management shall collaborate with department heads, determine key categories of products and services, and dedicate full-time managers (if needed) to coordinate the procurement of products and services.

B. REVIEW

F2OnSite shall conduct an annual review of the Purchasing Department to ensure compliance with this policy and assess the department's progress in achieving its purpose. Executive management shall, at a minimum, ensure annual reviews are conducted to assess progress against approved cost, schedule, and performance metrics.

C. ACQUISITION STRATEGY

With respect to the acquisition of products and services, a procurement action includes the following:

- Entry into a contract or any other form of agreement including, but not limited to, basic ordering agreements, blanket purchase orders, indefinite quantity, indefinite delivery contracts and other similar products and services.
- Issuance of an order or any transfer of funds to acquire a service on behalf of F2OnSite.

Requirements

The source of the requirement, the outcomes to be achieved, and, if performance based, the metrics used to measure the outcomes.

- How the requirement was previously satisfied.
- The nature and extent of research conducted.
- Determine if a benefit analysis was conducted.

Acquisition planning

- The adequacy of the acquisition approach including appropriate milestones.
- Cost and price estimate for the total planned acquisition.
- How the acquisition will be funded and the availability of funding.
- Technical, business, management, and other significant considerations.
- Any required waivers or deviations.
- Documentation to explain why full and open competition procedures do not apply.

Contract Award

- The type of business arrangements anticipated (single contract, multiple award, etc.).
- The duration of each business arrangement.
- Pricing arrangements (fixed price, reimbursements, time and materials, etc.) and deposits.

Risk Management

The Purchasing Department should prepare an assessment of current and potential technical, cost, schedule, and performance risks and plan for mitigating or retiring those risks.

Contract Tracking

The Purchasing Department, along with the requesting F2OnSite department, shall monitor existing or planned contract awards, quality assurance, and contract performance.

Performance Evaluation

The Purchasing Department shall establish procedures and guidelines for evaluating whether the metrics and any other measures identified to guide the acquisition have been achieved. These measures shall include the thresholds for cost, schedule, and performance for the acquisition of a product or service.

D. DATA COLLECTION REQUIREMENTS

The Purchasing Department shall establish procedures to collect the following types of data on acquisitions of products and services.

- The products and serviced purchased.
- The total estimate value of the contract.
- The type of contract (fixed price, time and materials, etc.).
- The department requesting the acquisition.
- The extent of competition in making the purchase and the number of offerors.
- Whether the acquisition was made from a small business concern, disadvantaged individuals, etc.
- Whether the acquisition considered environmentally friendly products and services.

E. IT PRODUCTS AND SERVICES

F2OnSite has agreed standards in place for desktop software, operating systems, computer networks, computer hardware and peripherals, and IT related services. This standardization is essential as it allows F2OnSite's IT Department to provide a quality and reliable service.

The main benefits are:

- IT Support Staff are familiar with hardware and peripherals, thus speeding up fault finding.
- The IT Department is able to stock standard spares in order to reduce down time.
- Network installations are planned and coordinated centrally by experienced network engineers.
- IT services with relevant skill sets provide F2OnSite with a competitive advantage.
- Security and privacy requirements can be met per regulations, industry guidelines, and best practices.

Approval Process

The IT Department is the sole authority for submitting requisitions for IT equipment on behalf of any department that has approval to obtain such equipment.

All IT related hardware and software will be specified by the IT Director. Hardware and software cannot be purchased without a completed IT procurement authorization form. This form needs to be completed and signed by the user's line manager. Upon receipt of the completed form, IT will record the request and the IT Director will make a decision whether to approve, decline or amend the requirements for the purchase of the IT related products and/or services.

- If the request is approved, IT will forward the request to the Purchasing Department for fulfillment.
- If declined or changed, the IT Director will provide a brief explanation to the requesting manager.

- Equipment suppliers may be recommended by the IT Department but may be changed on a periodic basis.

Product Delivery

The IT Department will request that equipment be delivered to the IT Department where it can be checked for damage and compliance with the ordered specification prior to being set up and transported to its final destination.

The IT Department will inform the original requestor of the equipment when the equipment is delivered to the IT Department, and will make arrangements for installation.

The IT Department has a standard set-up procedure for new hardware, software and systems. This procedure ensures the equipment is configured correctly and that all IT security measures are addressed. This includes the setup of passwords, anti-virus software, and security.

Installation of replacement equipment will be given priority over new equipment in order to maintain continuity in the existing service.

A program for the systematic monitoring and evaluation to ensure that standards of quality are being met shall be established for all software developed or acquired by F2OnSite. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security.

Management shall have a clear oversight capacity in the quality testing process with the final product being certified as:

- Fit for purpose - the product should be suitable for the intended purpose, and
- Right first time - mistakes should be eliminated prior to release.

Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the information system.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Vice Presidents, senior executives, the Purchasing Department, and the IT Department.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT APO01.03, APO01.11, APO03.06, APO03.08, APO09.05, DSS04.05, DSS05.02
GDPR Article 25
HIPAA 164.308(a)(1)(ii)(A)
ISO 27001 6.1.2, 7.1, A.12.1.2
NIST SP 800-37 2.8
NIST SP 800-53 3.11, CM-8, MP-6
NIST Cybersecurity Framework ID.SC1-2, DE.DP-2, RS.RP-1
PCI A3.1.2.b

ADMIN SPECIAL ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program.

II. Purpose

The purpose of this policy is to establish the rules for creating, using, monitoring, controlling, and removing accounts with special access privileges.

III. Scope

This policy applies to all Staff that have, or may require, special access privilege to any F2OnSite Information Resources.

IV. Policy

F2OnSite departments must submit to the IT Department a list of administrative contacts for their systems that are connected to the F2OnSite network.

All users must sign the F2OnSite non-disclosure agreement before access is given to an account.

All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization. Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the IT Director.

Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (e.g. user account vs. administrator account). Users with administrative account access shall use a dedicated or secondary account for elevated activities. This account shall only be used for administrative activities and not Internet browsing, e-mail, or similar activities.

Each account used for administrative/special access must comply with F2OnSite's Password Policy. The password for a shared administrator/special access account must change when an individual with the password leaves the department or F2OnSite, or upon a change in the vendor personnel assigned to the F2OnSite contract.

In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:

- Must be authorized
- Must be created with a specific expiration date
- Must be removed when work is complete

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all IT system administrators and security personnel.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, DSS05.02,
DSS05.07
GDPR Article 32
HIPAA 164.312(a)(2)(i)
ISO 27001 A.7.2.1, A.12.4.3
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 AC-2, AC-5, AC-6, AT-3
NIST Cybersecurity Framework PR.AC, PR.AT-2, DE.DP-2, RS.RP-1
PCI 2.2.4.a-c, 6.4.2, 7.1.1-2

AGREEMENT : BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement), is made as of _____, 20__ (the Effective Date), by and between F2OnSite (Covered Entity) and _____ (Business Associate), collectively termed the “Parties”, to comply with privacy standards adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, 45 C.F.R. parts 160 and 164 (“the Privacy Rule”) and security standards adopted by the U.S. Department of Health and Human Services as they may be amended from time to time, 45 C.F.R. parts 160, 162 and 164, subpart C (“the Security Rule”), and the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 and regulations promulgated there under and any applicable state confidentiality laws.

Business Associate provides services to or on behalf of Covered Entity. In connection with these services, Covered Entity discloses to Business Associate certain Protected Health Information (PHI) that is subject to protection under the HIPAA Rules and the HIPAA Rules require that Covered Entity receive adequate assurances that Business Associate will comply with certain obligations with respect to the PHI received in the course of providing services to or on behalf of Covered Entity. In consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Definitions. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, PHI, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured PHI, and Use. Specific definitions:
 - (a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103.
 - (b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103.
 - (c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
2. Obligations and Activities of Business Associate. Business Associate agrees to:
 - (a) Not use or disclose PHI other than as permitted or required by this Agreement or as required by law;
 - (b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

- (c) Provide to Covered Entity a description of Business Associate's Technical, Physical, and Administrative security safeguards that protect PHI;
- (d) Provide to Covered Entity a copy of annual auditor reports and test results of Business Associate's Technical, Physical, and Administrative Safeguards that protect PHI.
- (e) Report to Covered Entity within 72 hours any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR 164.410, and any security incident of which it becomes aware;
- (f) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;
- (g) Make available PHI in a designated record set to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;
- (h) Make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526;
- (i) Maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;
- (j) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and
- (k) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

- (a) Business Associate may only use or disclose PHI as necessary to perform the services set forth in Service Agreement. Business Associate is authorized to use PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c).
- (b) Business Associate may use or disclose PHI as required by law.
- (c) Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's minimum necessary policies and procedures.
- (d) Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 except for the specific uses and disclosures set forth below.
- (e) Business associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- (f) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of

the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.

- (a) Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. Permissible Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

6. Term and Termination

- (a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.
- (b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement including a breach of PHI.
- (c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:
 - 1. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to Covered Entity the remaining PHI that the Business Associate still maintains in any form;
 3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 4. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out in section "Permitted Uses and Disclosures By Business Associate" which applied prior to termination; and
 5. Return to Covered Entity the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
- (d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

7. Conflict. In the event of any conflict between the terms and conditions of this Agreement and the Services Agreement this Agreement shall prevail.

8. Severability. Every provision of this Agreement is intended to be severable. In the event any term, provision, covenant, or condition of this Agreement is declared to be illegal or invalid for any reason whatsoever by a court of competent jurisdiction, that illegality or invalidity shall not affect the other terms and provisions of this Agreement, which shall remain binding and enforceable.

9. Entire Agreement. This Agreement contains the entire understanding and agreement of the parties, and there have been no promises, representations, agreements, warranties, or undertakings by either party one to the other, either oral or written, of any character or nature, except as otherwise set forth in this Agreement.

10. Attorneys' Fees. In the event of a dispute regarding any provision of this Agreement, the prevailing party shall be entitled to collect reasonable attorneys' fees from the non-prevailing party.

IN WITNESS WHEREOF, the Parties hereby execute this Agreement to be effective as of the date written above.

COVERED ENTITY:
F2OnSite

By: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE:

[Business Associate Name]

By: _____

Title: _____

Date: _____

AGREEMENT : NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (Agreement), is made by and between F2OnSite (Company) and _____ (Employee), collectively termed the "Parties". The Parties agree as follows:

1. Employee will perform services for F2OnSite which may require F2OnSite to disclose Sensitive Information to Employee. Sensitive Information is information that is privileged or proprietary information which, if compromised through unauthorized disclosure, alteration, corruption, loss, or misuse could cause serious harm to F2OnSite. With respect to Sensitive Information, the Employee agrees to:
 - a. Hold Sensitive Information in strict confidence and shall exercise a reasonable degree of care to prevent unauthorized disclosure, alteration, corruption, loss, or misuse;
 - b. Not reproduce or replicate Sensitive Information nor use Sensitive Information commercially or for any purpose other than the performance of Employee's duties for F2OnSite.
 - c. Restrict disclosure of Sensitive Information solely to those individuals having a need to know, and not disclose Sensitive Information to any other party;
 - d. Advise associates (e.g. F2OnSite staff, service providers, suppliers) of their obligations with respect to the Sensitive Information;
 - e. Promptly disclose to F2OnSite of any requirement or request by any third person that Sensitive Information be disclosed pursuant to legislation, legal directive, public regulation, court decision or the like or in connection with the pursuit or defense of a claim in order to afford F2OnSite an opportunity to limit or restrict such disclosure or to obtain appropriate protective/secrecy orders with respect thereto and to obtain its agreement prior to further action.
2. Ownership. The Sensitive Information shall be deemed the property of F2OnSite and, upon request, Employee shall return all Sensitive Information to F2OnSite.
3. Rights. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Information disclosed by either party or in any intellectual property rights related thereto.
4. Disciplinary Action. F2OnSite reserves the right to take disciplinary action, up to and including termination, for violations of this Agreement.
5. Jurisdiction. This Agreement shall be governed by and construed under the laws of the State of California.
6. Severability. Every provision of this Agreement is intended to be severable. In the event any term, provision, covenant, or condition of this Agreement is declared to be illegal or invalid for any reason whatsoever by a court of competent jurisdiction, that illegality or invalidity shall not affect the other terms and provisions of this Agreement, which shall remain binding and enforceable.
7. Entire Agreement. This Agreement contains the entire understanding and agreement of the Parties, and there have been no promises, representations, agreements, warranties, or undertakings by either party one to the other, either oral or written, of any character or nature, except as otherwise set forth in this Agreement.
8. Attorneys' Fees. In the event of a dispute regarding any provision of this Agreement, the prevailing party shall be entitled to collect reasonable attorneys' fees from the non-prevailing party.

IN WITNESS WHEREOF, the Parties hereby execute this Agreement to be effective as of the date written below.

Employee:

By: _____

Name: _____

Date: _____

F2OnSite

By: _____

Name: _____

Date: _____

ANTI-MALWARE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

II. Purpose

The purpose of this policy is to describe the requirements for dealing with computer virus, worm, Trojan Horse, spyware, Ransomware, and other types of malicious software.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

The Chief Security Officer shall ensure:

- Procedures and tools exist to guard against, detect, and report malicious software. Centrally managed anti-malware software continuously monitors and defends Information Systems.
- IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software. Where possible, anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) shall be enabled in an operating system or deployed through appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.

- End users are aware of the security policies enforced on their workstations.
- Anti-virus software is installed at appropriate locations within organizational Information Systems including all systems commonly affected by malicious software (particularly personal computers and servers).
- Installed anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software including Ransomware.
- Systems considered to be not commonly affected by malicious software, receive periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
- Anti-virus mechanisms are properly maintained and kept current with the scanning engine and signature database updated every 12 hours per this policy.
- Periodic scans of the Information System shall be performed and audit logs generated and retained per Data Retention Policy requirements. Real time scan of files from external sources shall be performed as files are downloaded, opened, or executed.
- Devices are configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
- Anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. If anti-virus mechanisms are disabled, additional security measures may need to be implemented for the period of time during which anti-virus protection is not active.

All workstations whether connected to the F2OnSite network, or standalone, must use the F2OnSite IT approved virus protection software and configuration.

The virus protection software must not be disabled or bypassed.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server attached to the F2OnSite network must utilize F2OnSite IT approved virus protection software and setup to detect and clean viruses that may infect file shares.

Each E-mail gateway must utilize F2OnSite IT approved e-mail virus protection software and must adhere to the rules for the setup and use of this software.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Help Desk.

Mobile Code shall be authorized before its installation and use. Anti-malware software shall ensure:

- Authorized Mobile Code operates according to a clearly defined security policy.
- All unauthorized Mobile Code is prevented from executing.

Malware actions (e.g. anti-malware software updates, definition updates, malware infections, Ransomware attacks, etc.) shall be logged with logs retained for one year to allow proper investigations into malware related incidents.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff that use F2OnSite Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	UPDATED Initial policy release	D LAUDERBACK

References:

COBIT APO13.07, APO14.10, BAI04.05, BAI09.04, DSS04.05, DSS04.07, DSS05.02, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(5)(ii)(B)

ISO 27001 A.12.2

NIST SP 800-37 3.1

NIST SP 800-53 AC-19, PL-8, SC-3, SI-2-4

NIST Cybersecurity Framework DE.CM-4-5, RS.RP-1, RC.RP-1

PCI 5.1-4

APPLICATION IMPLEMENTATION POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

When new applications are developed, an impact analysis must be performed to ensure that existing Information Systems remain stable.

II. Purpose

This policy is designed to protect the organizational resources on the network by defining requirements for new applications. Assessments should be used to identify data classification and security levels, storage, and system requirements.

III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

IV. Policy

ABC Company Staff shall work with application developers and Chief Security Officer (MGMT) to assess data requirements for any new applications. Staff shall specify their requirements for the applications and application developers shall work with Staff to identify and categorize data according to Data Classification Policy.

Once the data and application requirements are established, the MGMT shall evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks. The MGMT, Staff, and application developers will work together to provide required and reasonable access capability to systems and data both during development and final project implementation while providing effective and sufficient controls at a reasonable cost. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

The data assessment, risk evaluation, and system requirements shall be performed early in the project life cycle since without this information, the overall cost of the project cannot be accurately assessed.

Where possible, IT Staff shall ensure that each server only provides one primary function. This helps prevent instances where separate functions require different security levels on the same device. IT Staff shall enable only necessary services, protocols, and daemons required by the application/system. IT Staff shall develop a baseline configuration for the application and system. Such configuration will be helpful in identifying unusual events and activities.

Prior to placing the application into production, and annually thereafter, a security audit shall be performed on the application. This helps ensure the security of the application, underlying host configuration, and data.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff that use ABC Company Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO05.03, APO05.05, APO12.02, APO12.07, BAI03.05-06, BAI03.09, BAI10.07
GDPR Article 25, 32
HIPAA 164.308(a)(7)(ii)(E)
ISO 27001 A.9.4, A.13.1, A.14
NIST SP 800-37 3.1
NIST SP 800-53 AC-6, CA-8, CM-2
NIST Cybersecurity Framework ID.AM, ID.BE-5, ID.GV-4, DE.DP-2
PCI 2.2, 6.1

APPROVED APPLICATION POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

To protect the security of F2OnSite Information Resources, all Staff must ensure that only approved applications are used.

II. Purpose

This policy is designed to protect Information Systems by requiring all Staff to only run application programs deemed safe by the IT department.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

The IT Department shall prepare and maintain a list of software applications that are approved for general use by F2OnSite Staff. The list of programs that appears on the approved list of software applications shall include general office products such as word processing, spreadsheet, and presentations as well as programs specific to a department or function (e.g. anti-malware).

Staff may use and operate programs that appear on the approved list of software applications. If a Staff member wants to use an application that does not appear on the approved list, the Staff member must submit a request to the IT department to evaluate the application. This process applies to licensed applications, shareware, freeware, trial programs, and other software. The IT Department will evaluate requests and update the approved list of software applications on an as needed basis.

Only approved software applications are allowed to access F2OnSite networks and Information Resources. Under no circumstances shall Staff use programs that are not

on the approved list of Software applications. Staff members who introduce a security issue by installing and running an unapproved program risk disciplinary action.

Special exceptions may be made to this policy for specific employees depending on the required job function and the skills of the employee. Some reasons for exception include:

- A Staff member who tests new applications on a test network and then on the main network
- A programmer that must run applications in order to test the software
- Network administrators who install and test software as a part of their regular job duties

On a periodic basis, software inventory tools shall be used to identify and classify software installed on Information Systems. See the Asset Management Policy for more information.

Where possible:

- Approved software applications shall be whitelisted to ensure that only authorized software can be executed
- Unauthorized software shall be blocked from executing on Information Systems

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff that use F2OnSite Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO01.02, APO01.06, BAI02.04, BAI06.01

GDPR Article 32

HIPAA 164.308(a)(7)(ii)(E)

ISO 27001 A.9.4

NIST SP 800-37 2.2, 3.5

NIST SP 800-53 AC-2, AC-3, AC-20, CA-6, CM-2, CM-11, PM-5, SA-1

NIST Cybersecurity Framework ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-3, DE.CM-1

PCI 6.4.5, 6.4.6, 12.3.4

ASSET MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to protecting its Staff, customers, partners and its operations. This policy enables F2OnSite to effectively deliver equipment and services that support company business processes.

II. Purpose

This policy protects F2OnSite's assets and helps ensure our ability to continue business operations.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

A. ASSET TYPES

The following types of devices shall be tracked assuming they meet the other requirements of this policy:

- Desktop workstations
- Firewalls
- Handheld devices
- Laptop mobile computers
- Memory devices
- Printers, Copiers, FAX machines, multifunction machines
- Routers
- Scanners
- Servers
- Software (application and operating system)

- Switches

B. ASSET VALUE

Assets which cost less than \$100 shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

- Hard Drives
- Temporary storage drives
- Tapes with data stored on them including system backup data

Although not specifically tracked, other storage devices including CD ROM disks and USB flash drives are covered by this policy for disposal and secure storage purposes.

C. ASSET MEDIA

Small memory storage assets will not be tracked by location. Instead, they will be tracked and inventoried by Data Owner. Enterprise software should be used that can configure systems to allow the use of small storage devices on specific Information Systems. These assets include:

- CD/DVD disks
- Memory sticks (USB flash drives)

If these types of devices are permitted for some Staff, the Data Owner of the device must sign for receipt of these devices in their possession. All Staff must also agree to handle memory sticks, and CD/DVD disks in a responsible manner and follow these guidelines:

- Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
- Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.
- The Memory Device Data Owner agreement allows Staff to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all Staff that will work with any organizational data when the Staff begins working for the organization. It will also be submitted when Staff receives one or more memory sticks, temporary storage drives, or data backup drives.

D. ASSET TRACKING REQUIREMENTS

All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.

An asset tracking database (Database) shall be created to track assets. It will include all information on the Asset Transfer Form including the date of the asset change.

The Database shall be maintained, accurate, and kept up-to-date. The Database shall include an inventory of all Information System assets that have the potential to store or process information. The inventory shall include all hardware and software assets, whether connected to the organization's network or not. Any unauthorized assets shall be removed, quarantined, or the inventory updated in a timely manner. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the Database. All assets maintained in the Database inventory must have an assigned owner.

Software applications and operating systems currently supported and receiving vendor updates shall be added to the Database. Unsupported software shall either be removed or classified as Unsupported in the Database.

E. TRANSFER PROCEDURE

Asset Transfer Checklist - When an asset type listed on the Asset Types list is transferred to a new location or Data Owner, the IT Asset Transfer Checklist must be filled out by the Data Owner of the item and approved by an authorized representative of the organization. The Data Owner is the person responsible for the asset. If the item is a workstation, then the Data Owner is the most common user of the workstation. For other equipment, the Data Owner is the primary person responsible for maintenance or supervision of the equipment.

The Data Owner must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new Data Owner, or being disposed. The following information must be filled in:

- Asset Type
- ID number
- Asset Name
- Asset Description
- Current Location
- Designated Data Owner
- New Location
- New Data Owner
- Locations of Sensitive Data

Approval - Once the Data Owner fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

Data entry - After the Asset Transfer Checklist is completed, it will be given to the Database manager. The asset tracking Database manager shall ensure that the information from the forms is entered into the Database within one week.

Database - An active discovery tool shall be used to identify devices connected to the network. Software inventory tools shall be used to identify and classify operating system and application software on such devices. The Database shall be updated based upon the results of the hardware and software inventory tools. Where possible, the Database shall be automatically updated through the use of automated tools. Resource Owners shall check the Database on a regular basis to ensure applicable assets are included in the Database.

F. ASSET TRANSFERS

This policy applies to any asset transfers including the following:

- Asset purchase
- Asset relocation
- Change of asset Data Owner including when an Staff leaves or is replaced
- Asset disposal
- In all these cases the asset transfer checklist must be completed

G. ASSET DISPOSAL AND REPURPOSING

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to tenant assignment or jurisdictional transport.

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. The manager of the user of the asset shall determine the level of maximum sensitivity of data stored on the device.

Below is listed the action for the device based on data sensitivity according to the data classification process:

- Public - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing
- Sensitive - Erase the data using any means such as reformatting or degaussing
- Confidential - The data must be erased using an approved technology to make sure it is not readable using special technology techniques approved by the Chief Security Officer.

H. MEDIA USE

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

- Memory stick/flash drive
- CD/DVD disk
- Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data classification process:

- Public - Data may be removed with approval of the first level manager and the permission is perpetual for the Staff duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
- Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
- Confidential - The data may only be removed from secure areas with permission of a Vice President or higher level of management. Staff shall document security precautions for both the transport method and at the destination.

I. SEPARATION OF DUTIES

Duties and job functions shall be separated to ensure Information Resource availability, confidentiality, and integrity.

J. CLEARING AND SANITATION

Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. Information Resources shall be sanitized before they are released from Sensitive Information controls or released for use at a lower classification level. Overwriting is no longer acceptable for sanitization of magnetic media. Only degaussing or physical destruction is acceptable.

K. PROTECTION MEASURES

Protection profiles required for a particular information system shall be determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals, and need-to-know.

Procedures shall ensure that the proper access and integrity controls prevent the improper alteration or destruction of data.

A transaction log, protected from unauthorized changes, shall document:

- The off-line verification of all changes
- The immediate correction of unauthorized data and Information System software changes

Procedures shall be implemented that:

- Define logical access controls where the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system
- Support this policy and its security mechanisms
- Define processes or mechanisms that allow users (or processes acting on their behalf) to determine the formal access approvals granted to another user
- Define processes or mechanisms that allows users (or processes acting on their behalf) to determine the sensitivity level of data

The Information System shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific entry point. The default shall be a single logon session.

The Information System shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the Securing Information Systems Policy.

If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

V. ENFORCEMENT

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. DISTRIBUTION

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO01.06, APO09.03, BAI09.01, BAI09.02-03, DSS04.07, DSS05.04-05, DSS06.06
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B)
ISO 27001 A.8, A.9
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 CM-8, PL-4
NIST Cybersecurity Framework ID.AM, PR.PT, DE.DP-2, DE.CM-1-2, RS.RP-1
PCI 1.1.5

AUDIT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Security controls and safeguards are part of F2OnSite's risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

Security audits help ensure that security controls are sufficient and effective at providing information confidentiality, availability, and integrity.

III. Scope

This policy applies to all Department Heads with authorized access to any of F2OnSite's Information Resources.

IV. Policy

Security audits help manage and reduce risks to F2OnSite's Information Resources. A security auditor, usually an independent third party, evaluates systems for security best practices and compliance with an established set of security requirements.

An independent security audit assists the Chief Security Officer (MGMT) in ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The MGMT shall:

- Resources – identify resources to perform the security audit.
- Scope – define the scope of the system being certified as well as its boundaries.
- Security Requirements – prepare a list of the security requirements that are relevant to the system.
- Description – Describe the system including mission description, system identification, criticality, etc. Document the environment including facilities,

physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

The MGMT shall consider the following when determining the audit scope:

- Vulnerabilities – establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact.
- Evaluating – identify methods for evaluating vulnerabilities and assigning risk ratings based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit sensitive data.
- Automated tools – automated tools may be used to identify a variety of vulnerabilities including weak passwords, configuration issues, improper access controls, and patch management issues.
- Administrative safeguards – the auditor can review and evaluate policies, procedures, training plans and other administrative security controls.
- Penetration testing – penetration testing may be used to identify system vulnerabilities. Examples of penetration testing include evaluations of firewalls and other network entry points, analysis of software applications and websites, and social engineering tests of Staff security education and awareness training.
- Internal vulnerability assessment – layers of defense help protect F2OnSite’s internal systems should the external network perimeter be breached. Internal vulnerability assessments identify weaknesses in the network.

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Where possible, the MGMT shall use Certified Information Systems Auditors to audit the security controls of F2OnSite’s Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The auditor's report shall include their project scope, findings, and recommendations to enhance security. The MGMT shall:

- Review the security auditor's report to confirm the findings and verify the security recommendations are sufficient and effective.
- Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The MGMT shall document important findings in the Audit Log Form and The Risk Management Officer shall provide necessary reporting to F2OnSite Executive Management.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads, MGMT, Risk Management Officer, and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT EDM03.02, APO01.03, APO01.11, APO12.02, APO12.07, MEA03.01, MEA04.11
GDPR Article 32
HIPAA 164.308(a)(8)
ISO 27001 9.2, A.15.2.1
NIST SP 800-37 3.5
NIST SP 800-53 3.3, AC-5, AU-6, CA-2
NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2
PCI 2.2.a-d

AUDIT TRAILS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Audit trails can help detect security violations, performance issues, and flaws in applications. They can also be used to help reconstruct or review Information Resource related activities.

II. Purpose

This policy establishes the framework for audit trails and their use as a technical control to help manage Information Resource related risks.

III. Scope

This policy applies to the IT Department and other departments responsible for acquiring, implementing, and maintaining Information Resources.

IV. Policy

A. PURPOSE

An Information Resources audit trail is a record of activities and events related to IT facilities, networks, servers, users, applications, and related assets. An Information Resource may have different types of audit trails each devoted to a particular activity.

Auditing includes the review and analysis of safeguards and controls. In many instances audit trails are used as record of activity. Auditing systems generally consist of:

- Logging – collecting and recording events
- Reporting – data analyzer and reporting

Often a file is used to transfer the audit data from the collector to the analyzer. This leads to problems when the audit data is collected from different systems. This is due to

the lack of a standard interface for audit trails. Developing standards for the format and content of audit trails is an ongoing research effort.

Audit trails can be used:

- To establish individual accountability – an individual's actions are tracked in an audit trail allowing users to be personally accountable for their actions. With user actions logged, audit trails help ensure accountability and Staff are less likely to perform unauthorized activities. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.
- Reconstruct events – audit trails can be used to reconstruct events after an incident has occurred. The amount of damage that occurred can be assessed by reviewing audit trails of system activity to identify how, when, and why the incident occurred.
- Resource monitoring (problem identification) – audit trails may also be used to detect disk failures, over utilization of system resources, network outages, and similar events.
- Intrusion detection – audit trails can help determine events that allowed unauthorized access to Information Resources. Intrusions can be detected in real time, by examining audit records as they are created or after the fact, by examining audit records in a batch process. Deploying, monitoring, and reporting are important intrusion detection considerations.

Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing F2OnSite's Information Resources. Audit trails can also be used as an incident detection and response mechanism to:

- Reconstruct a timeline of events that occurred
- Identify individuals involved
- Additional information for research into the extent of the damage
- Help ensure correction
- Resume normal business operations with minimal delay
- Use information from this incident to minimize or eliminate future events

The Risk Assessment Policy ensures that important assets are identified and the appropriate security controls are in place. Real time monitoring shall be used on important Information Resources to ensure their continued availability and integrity.

B. AUDIT TRAIL REQUIREMENTS

Information Resources shall automatically create and maintain audit trails or logs. Refer to the Logging Policy for more information on:

- Activities to be logged
- Elements of the log
- Log formatting and storage
- Log information security issues
- Where possible, audit trails shall include before and after versions of records that were modified. This allows F2OnSite to reconstruct events whether the event was made by a Staff member, a hardware malfunction, software bug, etc.

Audit trails created and maintained by the information system shall record changes to user formal access permissions. Monitoring and logging activities shall include the unique identification of each user and association of that identity with all auditable actions taken by that individual.

Information Resources clocks shall be synchronized to enable research and investigation activities.

Sensitive Information shall be sanitized before being written to log files.

Monitoring and logging activities shall be periodically tested by IT security Staff.

C. REVIEW AND ANALYSIS

Audit trails must be reviewed on a daily basis. Such review to include a review of:

- All security events
- Logs of all system components that store, process, or transmit sensitive information or could impact the security of sensitive information.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (e.g. firewalls, intrusion detection systems (IDS), intrusion-prevention systems (IPS), authentication servers, e-commerce redirection servers, etc.).
- Review of logs of other system components periodically based on F2OnSite's risk management strategy, as determined by the annual risk assessment.

Staff shall be assigned to follow-up on all exceptions and anomalies identified during the review process.

Log files shall be copied to a protected area and retained for at least one year to assist in future investigations and monitoring. At least three months of history shall be immediately available for analysis (e.g. on-line, archived, or restorable from backup).

The following must be considered when reviewing audit trails:

- Recognize normal activity – reviewers must know what to look for to be effective in spotting unusual activity. They need to understand patterns and activity of normal traffic.
- Recognize unusual activity – Staff shall review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this requirement.
- Contain a search capability – audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.
- Follow-up reviews – the appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.
- Develop review guidelines – application owners, data owners, system administrators, data processing function managers, and computer security managers must determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.
- Automated audit analysis – analysis and reporting shall be performed using automated tools on a scheduled basis. Monitoring systems and logs shall be reviewed and analyzed in a timely manner. Log files related to file integrity, IDS, IPS, authentication, and authorization systems shall be reviewed and analyzed daily.

D. SECURITY CONSIDERATIONS

The contents of audit trails shall be protected against unauthorized access, modification, or deletion. IT security Staff must protect the audit trail from unauthorized access. The following precautions must be taken:

- Control online audit logs. Access to online audit logs must be strictly controlled.
- Separation of duties. The Company strives for separation of duties between various personnel who administer the access control function and those who administer the audit trail.
- Protect confidentiality. The confidentiality of audit trail information must be protected if, for example, it records personal information about users.

Access to monitoring systems and log files shall be restricted to authorized personnel and protected against unauthorized alteration. File integrity monitoring or change detection software shall issue alerts upon unauthorized modification of:

- Critical system files
- Configuration files

- Log files

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all IT Department personnel and other F2OnSite Staff members responsible for acquiring, implementing, and maintaining Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT EDM02.03, EDM03.02, APO01.11, APO12.07, BAI04.05, MEA03.01, MEA04.11
GDPR Article 30, 32
HIPAA 164.308(a)(1)(ii)(D)
ISO 27001 A.12.4, A.15.2
NIST SP 800-37 3.7
NIST SP 800-53 3.4, AU-12, AU-13
NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2
PCI 6.3, 6.4.6, 10

BACKUP PLAN

I. Purpose of the Backup Plan

The purpose of this Backup Plan (Plan) is to document the processes related to backing up of F2OnSite's Information Systems, storing of backup information, testing of backups, and security related to backups.

II. Overview of the Backup Plan

This Plan documents our structured process of ensuring system availability and our ability to recover Information Systems from backups. Backups are used to provide corrective action against various types of threats including:

- Human error – a user accidentally deletes a file.
- Malicious software – a virus deletes files or corrupts systems and data.
- Intentional actions – a hacker deletes files.
- Hardware failure – a hard drive fails and files must be deleted.
- Application processing errors – a database is corrupt and must be restored.
- Facility issues – a fire, water pipe, or electrical surge damages equipment.

This Plan was developed to ensure:

- Business recovery objectives can be achieved.
- Backup solutions are scalable and can adapt to a changing business environment.
- Backups are robust and can be used to restore information when needed.
- Responsibility for ensuring sufficient and effective backups.
- Information systems and related data are properly identified so that they can be backed up.
- The location of backups has been properly identified along with the individuals who have access to the backups.
- Procedures to restore systems from backups are complete and maintained.
- Backups are periodically tested to ensure they are reliable and contain the necessary information.

F2OnSite's Backup Policy provides direction and guidance to this Plan and related activities.

III. Business Continuity Objectives

F2OnSite is committed to protecting its business operations, investments by its stakeholders, and assets of the organization. Risks assessments are used as a tool to help identify and mitigate risks to assets. F2OnSite's Risk Assessment Policy specifies that the risk assessment, risk analysis, and risk treatment plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks.

Our recent risk assessment identified important Information Systems. Our most recent Business Impact Analysis, part of our business continuity process, identified important Information Systems as well as our required recovery time objectives (acceptable downtime) and recovery point objectives (acceptable data loss).

Backups are an important part of providing Information System availability and are critical to F2OnSite's business continuity. Per the Backup Policy, the Chief Security Officer (MGMT) has performed a review and analysis of our Business Impact Analysis and costs and determined that F2OnSite shall operate at Tier 2: Data backups with hot site. See the Backup Policy for more information about the recovery Tiers.

IV. Responsibilities

The IT Director has been assigned the responsibility of implementing and managing F2OnSite's Backup Plan and related processes and procedures. The IT Director delegates some or all of the following backup related responsibilities to a Backup Coordinator:

- Requirements – systems to be backed up, acceptable downtime, acceptable data loss.
- Documentation – maintain a record of backup related documentation including flow charts, locations of backups, use of backup/recovery third party service providers, backup requirements, individuals with access to backup media, personnel contacts, etc.
- Procedures – backup procedures used to ensure business continuity and recovery objectives are achieved.
- Integrity – review testing of backups to ensure they are complete, reliable, and error free.
- Recommendations – recommendations to enhance the Backup Policy and/or Plan.

The IT Director periodically reviews the most recent Business Impact Analysis and the above information maintained by the Backup Coordinator to ensure:

- Backup solutions meet recovery Tier and Business Impact Analysis requirements.
- Backup solutions are scalable and can adapt to a changing business environment.
- Backup are robust and can be used to restore information when needed.
- Information systems and related data are properly identified so that they can be backed up.
- The location of backups has been properly identified along with the individuals who have access to the backups.

On an annual basis the IT Director makes available to Data Owners an overview of the Backup Procedures to make them aware of recovery times and possible data loss. Data Owner concerns are brought to the attention of the MGMT as a part of the annual evaluation of the recovery Tier, data loss and recovery time implications, and related costs.

V. Backup Procedures

A. OVERVIEW

The IT Operations Department is responsible for developing and maintaining backup procedures. Such procedures include:

- Scheduling backups and troubleshooting backup issues.
- Monitoring backups and related log files.
- Documenting backup success/fail.
- Notifying the System Administrator of any issues that require attention (e.g. failed backups, capacity issues, time to backup files, etc.).
- Defining procedures and creating documentation for sending backups off-site.
- Maintaining the Backup Log Form of all backup media including their location and, if off-site, when backup is expected to return on-site.

F2OnSite performs a full back up each evening for all important systems identified in the Business Impact Analysis. This ensures:

- *Integrity.* Since all important systems are backed up at the same time, transaction integrity between databases is achieved.
- *Recovery time.* Since all backups are full backups, no incremental backups are performed. This speeds recovery times as IT Operations Staff does not need to first restore from a full backup and then restore files from one or more incremental backups.

Full backups have the following constraints that are monitored by IT Operations Staff and the Backup Coordinator:

- *Capacity.* Since backups run unattended without operators present, sufficient storage capacity needs to be allocated for backups/media.
- *Time.* Backups generally start in the evening. To ensure integrity, they must complete before Staff returns to work the next day.

B. ARCHIVING AND RETENTION

F2OnSite employs a robust backup and archiving scheme that protects against malware and other types of threats. A minimum of 14 backups are maintained at any point in time. Exhibit A – Archiving and Rotation Schedule documents our labeling, archiving, and rotation schedule.

Examples of backups:

- Monday – each Monday IT Operations will use the Monday backup. This backup is retained on-site. This media is overwritten the following Monday.
- 1st Friday – the 1st Friday of the month IT Operations uses the Friday 1 backup. The following work day it is taken to off-site storage. This backup is returned to IT Operations

when the 2nd Friday backup is stored off-site. This backup is overwritten the 1st Friday of the following month.

- Month 1 – monthly backups are stored off-site until they are needed. IT Operations creates the Month 1 backup the last working day of the first month of each quarter (January 31, April 30, July 31, October 31). The following work day Month 1 is taken to off-site storage where it remains until it is needed again.
- Quarter 1 - quarterly backups are stored off-site until they are needed. IT Operations uses the Quarter 1 backup the last working day of each quarter (March 31, June 30, September 30). The following work day it is taken to off-site storage where it remains until it is needed again.
- Year end – year end backups are created the last working day of the year. They are stored off-site and retained per the Data Retention Policy. Year end backups are not overwritten or reused.
- Special – the IT Director may occasionally authorize Special or one-time backups be created. Examples include backups prior to IT hardware/software upgrades and moving equipment that contains important systems or data as identified in the Business Impact Analysis. IT Operations Staff is responsible for creating Special backups that contain retrievable exact copies of systems.

C. OFF-SITE STORAGE

The MGMT has determined that risks due to human error, hacker, equipment failure, or database integrity issues are more likely than environmental issues such as fire or flood. As a result, the IT Director has specified, with the approval of the MGMT, that the most recent backups be stored on-site.

- Monday through Thursday backups are always maintained on-site and reused the following week.
- Friday backups are rotated off-site. Only the most recent Friday backup is stored off-site. The remaining Friday backups are stored on-site.
- Monthly backups are stored off-site until they are needed and ready to be overwritten.
- Quarterly backups are stored off-site until they are needed and ready to be overwritten.
- Year end backups are stored off-site until disposal (never overwritten).

D. DISPOSAL PROCEDURES

Backups are retained according to Section V.B. Archiving and Retention. When backups are no longer needed and/or reach the end of their useful life, they are disposed of per F2OnSite's Disposal Policy.

E. TESTING BACKUPS

Testing provides assurance that backups are complete and error free. Testing can identify the following types of problems and issues:

- Inability to restore from older media (size, poor quality, too old, not properly stored).
- Current backup software cannot read old backups.
- Applications or data were not stored on original backups.
- Encryption or key management issues (can't read encrypted backups).

Twice each year the IT Director authorizes a test of backups and backup procedures. IT Operations Staff prepares a Test Case Scenario including:

- Test objectives – systems and/or applications to be tested.
- Tasks – detailed tasks needed to perform the test.
- Resources – resources required including timeframe, Information Systems, Staff (IT and users), backups, anticipated costs, etc.
- Validation – expected outcomes and validation processes.

Once the Test Case Scenario is approved by the IT Director, IT Operations Staff:

- Schedules – reserves Information Systems for testing and coordinates with user departments (if needed).
- Documentation – assembles system restore documentation, flowcharts, and any other documentation needed by IT Operations Staff.
- Resources – assembles backups used for the Test Case Scenario.
- Restore – restores systems according to documented procedures and the specific Test Case Scenario.
- Validation – documents actual events and compares with expected outcomes. Performs validation procedures identified in the Test Case Scenario. Involves users as needed to validate a successful restore.

Within one week of testing, IT Operations Staff prepares and delivers a report to the IT Director. Such report includes:

- An overview of the Test Case Scenario.
- Expected outcomes.
- Actual outcomes and other variances.
- Recommendations to enhance backup and recovery processes.

Based upon the testing results, the IT Director may recommend changes to the Backup Policy, this Plan, and/or backup/recovery procedures.

VI. Storage of Backups

A. ON-SITE BACKUPS

Backups that are stored on-site are located in a safe and secure room restricted to IT Operations Staff, the IT Director, and Backup Coordinator (collectively termed Authorized Individuals). The list of Authorized Individuals is reviewed by the IT Director at least annually to ensure it is relevant and sufficient.

To meet the specified Recovery Time Objectives outlined in the Business Impact Analysis, on-site backups are immediately available to Authorized Individuals.

Backups are encrypted to protect against theft and unauthorized access.

B. OFF-SITE BACKUPS

Backups stored off-site meet the following requirements:

- Annual review by IT Director or designate to ensure the environment is suitable for storing F2OnSite backups.
- Backups are encrypted to protect against theft and unauthorized access.
- Backups are stored in a safe and secure environment.
- Access to backups is restricted to authorized personnel approved by the IT Director or designate.
- The off-site environment allows F2OnSite to meet or exceed specified Recovery Time Objectives outlined in the Business Impact Analysis.

Off-site backup/recovery third party service providers are cleared to handle the highest level (see Data Classification Policy) of information stored.

Exhibit A – Archiving and Rotation Schedule

Label and Description	Retention	Location
Monday – backup performed each Monday	1 week	Always on-site
Tuesday – backup performed each Tuesday	1 week	Always on-site
Wednesday – backup performed each Wednesday	1 week	Always on-site
Thursday – backup performed each Thursday	1 week	Always on-site
Friday 1 – backup performed 1 st Friday of each month	1 month	Rotated off-site
Friday 2 – backup performed 2 nd Friday of each month	1 month	Rotated off-site
Friday 3 – backup performed 3 rd Friday of each month	1 month	Rotated off-site
Friday 4 – backup performed 4 th Friday of each month	1 month	Rotated off-site
Friday 5 – backup performed 5 th Friday of each month	1 month	Rotated off-site
Month 1 – backup performed end of month, 1 st month of quarter	3 months	Stored off-site
Month 2 – backup performed end of month, 2 nd month of quarter	3 months	Stored off-site
Quarter 1 – backup performed last day of 1 st quarter (March 31)	1 year	Stored off-site
Quarter 2 – backup performed last day of 2 nd quarter (June 30)	1 year	Stored off-site
Quarter 3 – backup performed last day of 3 rd quarter (Sept 30)	1 year	Stored off-site
Year End – backup performed on December 31	7 years	Stored off-site
Special – OS upgrades, data conversions, moving equipment, etc.	Varies	Always on-site

BACKUP POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Electronic backups are a business requirement to enable the recovery of data and applications in the case of natural disasters, system disk drive failures, espionage, data entry errors, viruses, or system operations errors.

II. Purpose

The purpose of this policy is to establish the rules for the backing up and storage of backups containing F2OnSite's electronic information.

III. Scope

This policy applies to all Staff that are responsible for the installation and support of IT, individuals charged with IT Security, and data owners.

IV. Policy

Backups are used to provide corrective action against various types of threats including:

- Human error - accidental deletion of files
- Malicious software – viruses delete or corrupt systems and data
- Intentional actions – a hacker deletes files
- Hardware failure – a hard drive fails and files must be deleted
- Application processing errors – database must be restored
- Facility issues – a fire, water damage, or electrical surge damages equipment

Backups are an important part of providing Information System availability and are critical to F2OnSite's business continuity. The Chief Security Officer (MGMT) will determine the risks related to Information Systems and will evaluate the following tiers to determine the appropriate Tier for F2OnSite given our Business Impact Analysis,

recovery time objectives (how much downtime is acceptable), recovery point objectives (how much data loss is acceptable), and costs:

- Tier 1: Data backup with no hot site - systems are backed up and the media is sent to an off-site storage facility. Without a hot site, recovery may require weeks or months. Manual or additional processes are needed to continue business operations.
- Tier 2: Data backup with a hot site – contains the elements of Tier 1 plus a hot site provides the required hardware and operating systems to allow recovery from the backup media. Recovery can typically be achieved in one to two days depending upon the extent of damage, activation of hot site, and restore time.
- Tier 3: Electronic vaulting - contains the elements of Tier 2 plus mission critical data is electronically vaulted where data is transmitted to another secure location (typically off-site) via a network or communication link rather than via portable media. Recovery can typically be achieved in less than one day.
- Tier 4: Point-in-time copies (images) - key systems are copied to disk according to a pre-determined schedule. In this Tier either an off-site facility receives encrypted disks or the point in time copies (images) are used to supplement traditional encrypted backup media sent off-site. Imaging enables the quick recovery of an entire system. Depending upon the type of disruption, recovery may require several hours up to one day.
- Tier 5: Transaction integrity - software applications are coded to ensure transactions are fully complete with integrity. This ensures consistency of data between production and recovery systems. Recovery may be able to be achieved in less than one hour.
- Tier 6: Near zero data loss - robust business continuity solutions maintain the highest levels of data currency and allow quick access to data. Solutions have no dependence on the applications and may require some form of disk mirroring or synchronizing solutions. Recovery may be achieved in less than an hour with almost no loss of data.
- Tier 7: Highly automated, business integrated solution - contains the elements of Tier 6 plus automation. Restoring of systems, applications, and data is automated. This Tier may involve data replication to a redundant data center. Recovery may be achieved in a few minutes with almost no loss of data.

Once the appropriate Tier has been identified, the Chief Security Officer shall ensure:

- F2OnSite's Backup Plan identifies procedures to implement the requirements of this policy and the appropriate Tier.
- All system data is automatically backed up on regular basis.

- Documentation identifies the location of sensitive information to ensure that it can be backed up.
- Documentation includes all important sources of data such as accounting systems, electronic records, diagnostic images, and other documents created or used.
- Procedures create and maintain retrievable exact copies of information.
- The frequency and implementation of backups is appropriate according to the requirements of the selected Tier.
- Backups are stored and transmitted in a safe and secure manner and comply with the requirements of the selected Tier.
- Backups are encrypted to ensure information confidentiality. This includes remote backups and cloud services.
- All backups have at least one offline (i.e., not accessible via a network connection) backup destination
- Procedures specify when a retrievable, exact copy of sensitive information must be created before movement of equipment.
- Procedures identify who is responsible for creating a retrievable exact copy of sensitive information before movement of equipment.

The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the data owner. The IT backup and recovery process for each system must be documented and periodically reviewed.

Vendor(s) providing off-site backup storage and recovery solutions must be cleared to handle the highest level of information stored.

Physical access controls implemented at off-site backup storage and recovery locations must meet or exceed the physical access controls of the source systems. Backups must be protected in accordance with the highest sensitivity level of information stored.

A process must be implemented to verify the success of the electronic information backup. Backups must be periodically tested to ensure that they are recoverable.

Signature cards held by the off-site backup storage and disaster recovery vendor(s) for access to backups must be reviewed annually or when an authorized individual leaves F2OnSite.

Procedures between F2OnSite and the off-site backup storage and disaster recovery vendor(s) must be reviewed at least annually.

Backups must have at a minimum the following identifying criteria that can be readily identified:

- System name
- Creation date
- Classification
- F2OnSite contact information

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT management, IT system administrators, and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT EDM03.02, APO12.02, APO12.07, APO13.07, DSS04.05, DSS04.05, MEA03.03

GDPR Article 25, 32

HIPAA 164.308(a)(7)(ii)(A)

ISO 27001 A.12.3

NIST SP 800-37 Appendix D

NIST SP 800-53 AU-9, CP-6, CP-9, CP-10

NIST Cybersecurity Framework PR.IP-4, RS.RP-1, RC.RP-1

PCI 9.5.1, 10.7, 12.10.1

BLUETOOTH POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite's Information Systems must be protected from communications related threats. Staff must use secure Bluetooth communications procedures.

II. Purpose

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances using short-wavelength radio transmission. The purpose of this policy is to ensure F2OnSite Information Systems are protected from Bluetooth communications threats.

III. Scope

This policy applies to F2OnSite Staff that use Bluetooth technology to connect to Information Resources.

IV. Policy

A. DEVICES

To be deployed on F2OnSite's Information Systems, Bluetooth devices must meet current Bluetooth specifications. Any exceptions require written authorization from the Chief Security Officer (MGMT). Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

B. SECURITY

Due to continuous communications between devices, unauthorized individuals may be able to track devices and decode information using sniffers or smart phones. Bluetooth connectivity threats include device tracking, eaves dropping, and man-in-the-middle attacks. Staff shall follow the following security requirements specified in this policy to minimize Bluetooth related risks.

Staff shall ensure devices use the strongest Bluetooth security available. Staff shall select devices that use Security Mode 3 or higher. These devices ensure authentication and encryption is established before the physical link is complete. In addition, traffic is encrypted in both directions.

The MGMT shall establish and maintain Bluetooth security guidelines. The Bluetooth security guidelines will include a list of approved Bluetooth technologies, types of information that may be transferred over Bluetooth, and requirements for selecting and using Bluetooth personal identification numbers (PINs).

Security training and awareness programs shall make Staff aware of Bluetooth security responsibilities and include:

- Steps to protect Bluetooth devices from loss or theft
- Pairing the Bluetooth devices only when needed
- Configuring the Bluetooth device to use the hidden mode
- Keeping devices turned off when not needed
- Updating device firmware when new releases are issued
- Unauthorized use or modification of Bluetooth devices

C. USER RESPONSIBILITIES

All Staff who use Bluetooth technology must comply with this policy. Staff shall refer to the list of approved Bluetooth technologies for appropriate hardware, software, and connectivity requirements. Only Bluetooth technologies specifically authorized are permitted to be deployed or connected to F2OnSite owned equipment.

When dealing with Bluetooth technologies and related equipment, Staff shall follow instructions outlined in F2OnSite's security training and awareness programs. Staff must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment. Staff shall report any misuse, loss, or theft of Bluetooth devices or systems immediately to IT security Staff.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO12.02, APO12.07, APO14.02, BAI10.07, DSS01.05

GDPR Article 25, 32

HIPAA 164.312(e)(2)(i), 164.312(e)(2)(ii)

ISO 27001 7.4, A.13

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 2.1, AC-4, AC-19

NIST Cybersecurity Framework ID.BE-4, PR.PT-4, DE.DP-2, DE.CM-3

PCI 1.3.4, 4.1, 6.5.4

BRING YOUR OWN DEVICE AND TECHNOLOGY POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Many Staff have personal hardware devices, software applications, utilities, tools, software development kits, and related products that do not meet F2OnSite's security requirements.

II. Purpose

The purpose of this Policy is to establish the rules for the use of Staff owned devices and technologies that utilize and access F2OnSite Information Resources.

III. Scope

This policy applies to all F2OnSite Staff that utilize Staff owned devices and technologies that utilize and access F2OnSite Information Resources.

IV. Policy

While F2OnSite has a Bring Your Own Device (BYOD) and Bring Your Own Technology (BYOT) culture, risks related to these devices must be managed.

On an annual basis the IT Department shall survey F2OnSite Staff about devices, operating systems, applications, browsers, tools, utilities, scripts, software development kits, cloud services, and related technologies used. The IT Department shall perform a BYODT analysis to determine:

- If the devices and/or technologies used pose a risk to F2OnSite's Information Systems.
- Changes or configurations necessary to minimize risks to F2OnSite's Information Resources.
- Mandatory security components (e.g. firewall, anti-malware protection, passwords, browser security settings, patch management, encryption, physical controls)

needed as a condition for allowing BYODT devices and technologies to access F2OnSite Information Resources.

- Prohibited devices and technologies.
- Devices and technologies allowed to access F2OnSite's Information Resources.
- Level of access (e.g. restricted, full, guest, admin) granted to the devices and technologies.
- Staff permitted and not permitted to use BYODT devices and technologies.

The IT Department shall implement controls that mitigate risks:

- The IT Department shall ensure Staff access to sensitive data from BYODT devices and technologies have strict password and encryption controls in place. See the Encryption Policy for more information.
- Anti-malware software shall be used and updated on a regular basis. See the Anti-Malware Policy for more information.
- In some instances, the IT Department may identify applications that, due to their sensitive nature, may not be accessed by Staff BYODT devices and technologies.
- Limit Staff activities performed on BYODT devices and technologies (e.g. no access to personal e-mail or social media).
- The IT Department may restrict access to F2OnSite Information Resources based upon Staff position responsibilities, geographical location, and lack of management approval.
- The IT Department will keep the Chief Security Officer (MGMT) informed of BYODT threats so that the security awareness and training program can be updated.

In the event a device is lost or stolen, the IT Department shall quickly block access to Information Resources from the device. In addition, the IT Department shall:

- Wipe F2OnSite data and applications, and/or
- Wipe the entire BYOD device if deemed necessary to ensure the security of F2OnSite Information Resources. Wiping the entire BYOD device may have Staff implications including the inability to make calls, loss of contacts, need to have the device restored, etc.

F2OnSite shall not be held liable for the loss of use or restoring of device, operating system, software applications, tools, scripts, data, etc. Staff should take the proper precautions (e.g. physical controls over devices, backing up of contacts and files, etc.) to minimize any disruptions.

BYODT devices and technologies shall employ controls that meet the following requirements:

- Password required at start up (power on).
- Inactivity timeout (per the Access Control Policy).
- Password change frequency (per the Password Policy).
- Safeguards ensure only approved users of BYODT devices and technologies can access F2OnSite Information Resources.

Staff shall not:

- “Root” or “jailbreak” a BYODT device and technology to free it from pre-defined limitations. This process modifies the system files and can result in an unstable and insecure device.
- Modify BOYDT device and technology hardware and/or software beyond installation of updates provided by the device maker or service provider.
- Disable BYODT device and technology protection systems including passwords, encryption, firewalls, and anti-malware without the approval of the IT Department.

The IT Department shall prepare a list of authorized BYODT devices and technologies that are allowed to utilize and access F2OnSite's Information Resources. In addition, the IT Department shall specify specific configurations and circumstances under which BYODT devices and technologies may connect to F2OnSite's Information Resources.

Per the Mobile Device Policy, only IT Department approved portable computing devices may be used to access F2OnSite networks and Information Resources. Per the Smartphone Policy, only IT Department approved Smartphones may be used to access F2OnSite networks and Information Resources. Per the Approved Application Policy, only approved software applications are allowed to access F2OnSite networks and Information Resources.

Staff shall be responsible for adhering to the requirements of this Policy. Staff shall notify the IT Department when:

- A new BYODT device or technology is acquired and needs access to F2OnSite Information Resources.
- A BYODT device or technology is taken out of service and is no longer used.
- The Staff member's role changes requiring a change in access (e.g. Staff member changes positions, Staff member on a leave of absence).

When choosing an appropriate plan, Staff should consider the additional voice minutes and data traffic that may be incurred. Except as otherwise consistent with this Policy, F2OnSite does not assume any financial responsibility for BYODT devices or technologies. F2OnSite shall not reimburse Staff for the following expenses:

- BYODT device or technology initial cost, maintenance, or replacement
- Recurring costs related to voice and data usage, roaming, etc.

- Connectivity charges including Wi-Fi hotspots usage
- Insurance
- Expenses related to restoring BYODT devices or technologies if lost, corrupted (e.g. Malware, incompatible applications, changes to operating system), or damaged.

F2OnSite shall reimburse Staff for the following expenses related to BYODT devices or technologies:

- Approved app software for use with corporate systems (e.g. e-mail apps).
- Approved anti-malware software.
- Approved encryption software for use with corporate systems (e.g. VPN software).

The F2OnSite IT Department shall perform periodic risk assessments to identify, manage, and reduce BYODT device and technology related risks and access to Information Resources. Refer to the Risk Assessment Policy for more information.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from BYODT devices and technologies which are generally higher-risk than non-portable devices (e.g., desktop computers).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO12.02, APO12.07, APO14.02, BAI10.07, DSS01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-2, ID.GV-4, ID.RA-1, ID.RA-4, PR.AC, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2

BUSINESS CONTINUITY BUSINESS RESUMPTION PLAN

I. Purpose of the Business Resumption Plan

The purpose of the Business Continuity Business Resumption Plan (Plan) is to address the restoration of business processes after an emergency. This Plan, along with the Business Continuity Communications Plan, supports the Business Continuity Disaster Recovery Plan to ensure the continuity of critical processes throughout an emergency or disruption. F2OnSite's Business Continuity Policy provides overall guidance and direction for business continuity planning and related activities.

II. Overview of the Business Resumption Plan

F2OnSite has a large variety of processes whose continuous operations are critical to the organization's continuing viability. Business resumption planning involves arranging for emergency operations of these critical business functions and for resource recovery planning of these functions following a natural or man-made disruption.

This Business Continuity Business Resumption Plan is only one component of F2OnSite's business continuity planning process. Business resumption plans are needed for all organizational units and include the logistics of getting personnel to work locations, temporary offices, recovery facilities, and housing. Employee safety orientation and insurance programs must also be included in business resumption planning.

F2OnSite's business resumption plan contains:

- Backup resource arrangements
- Procedures for notification, activation, mobilization, and emergency operations
- Resources at all facilities (permanent and temporary)

III. Preparing For A Disaster

A. INFORMATION NEEDED BEFORE A DISASTER

A formal Plan is needed for orientation of employees that will be involved in activating the plan and performing emergency operations. Orientation material is also needed for all employees in both the life safety and Plan areas. Detailed emergency operations plans are needed:

- Before a disaster for use during testing
- After a disaster for use during emergency operations

F2OnSite's departments shall prepare the following:

- *Off-site contingency site.* F2OnSite's Emergency Action Facilities Team shall arrange an off-site contingency site with work areas, conference rooms, and offices. The off-site contingency site can be utilized by F2OnSite employees until existing facilities are restored to normal operations or new facilities are available for occupancy.
- *Activation.* Departments should create documented activation and mobilization procedures.
- *Recovery documents.* While the IT Department is responsible for off-site storage of electronic data, all F2OnSite departments should evaluate manual recovery documents such as paper based data, forms, and procedures that must be stored off-site. F2OnSite departments will make the appropriate arrangements to ensure manual recovery documents, special forms, checks, etc. are stored off-site. These documents assist the individuals departments and minimize a business disruption.
- *Contact lists.* Departments should maintain emergency contact notification lists of all staff in their respective areas.
- *Supporting information.* In addition to the above, each department should maintain information, as appropriate, to assist in recovery operations. Backup resources such as locations and functions should be identified.
- *Testing* Testing and training procedures should be developed.

B. INFORMATION NEEDED DURING A DISASTER

- *Employee emergency reference cards.* Wallet size cards can be distributed to all employees. They contain both life-safety and information such as assembly locations, emergency operations policy, and numbers to call for information.
- *Notification/Activation reference cards.* Fold over pocket size cards contain a management call-tree, key assembly and backup resource addresses and telephone numbers, and emergency team contact information.
- *Team emergency operations procedures.* Detailed team operations procedures are normally needed only when multiple locations performing the same business function exist. Such locations require detailed procedures since they are normally not staffed

with the senior personnel needed to adapt policy level directives to the specifics of a particular emergency. This type of procedure is lengthy and difficult to prepare since it must anticipate various types and levels of disasters.

- *Team emergency reference cards.* Fold over pocket size cards contain the team member call-tree, an activity checklist, and backup resource information. Typical teams include: policy, emergency operations center, facility management, site recovery, backup data center operations, logistics, off-site storage coordination, floor wardens, assembly site coordinators, public/employee communications, telecommunications, etc.
- *Resource tabulations.* These tabulations contain such information as: lists of all resources by location including replacement information and backup resource locations; where all personnel are to report during emergency operations; and where to forward data and materials from off-site storage.

IV. Disaster

A. DISASTER NOTIFICATION

In the event of an emergency or disaster, the following notifying procedures must be followed:

- The Emergency Coordinator should initiate the notification process as soon as possible. If no operations personnel are on duty, management has been provided with the proper procedures and must notify the Emergency Coordinator who will then initiate the notification process.
- The Emergency Coordinator is at the top of the Emergency Notification List. If the Emergency Coordinator cannot be reached, the Alternate Emergency Coordinator must be contacted.
- The first member of the Readiness Team notified is responsible to notify other members of the Readiness Team and to initiate action. The initial action will be to assemble the Readiness Team at the Emergency Control Center or the Alternate Emergency Control Center.
- The Emergency Coordinator will make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.
- Based on the Readiness Team's assessment of the situation, the Emergency Coordinator will determine the severity of the problem and decide on the appropriate action.
- The appropriate correction or recovery plans will be implemented according to the severity of the emergency or disaster.

B. ADMINISTRATIVE TEAM

The Administrative Team will determine the procedures for all administrative assistance regarding hotel arrangements, flight schedules, etc.

Administrative Coordinating Procedures

- Work with Company management to determine extent and duration of resources needed.
- Identify locations and individuals involved.
- Gather and provide the necessary resources.

C. USER DEPARTMENT RESPONSIBILITIES

F2OnSite Company management will direct staff to implement emergency procedures. In most disaster situations, data will be lost. Departments must re-create lost data in addition to continuing existing business operations.

The Emergency Action Applications Team will coordinate with users and assist in identifying data that needs to be re-created. The Emergency Action Applications Team will also monitor recovery progress to ensure systems are operating correctly.

After the department personnel have been deployed, the department managers should track the location of their employees and continue to update the information throughout each day of the recovery operation.

User departments will create a log of daily events and tasks performed. This log will aid in recovery efforts as well as assist in a post disaster review of events.

Department managers should prepare written status reports on a frequent basis and, as requested by company management, to keep them apprised of the current status

As progress continues during the recovery operation, departments should be prepared to move back to the affected facility and resume normal business operations.

V. Procedures for Returning to Normal Operations

The following procedures are for returning to normal operations after emergency (recovery) operations.

A. EMERGENCY ACTION TEAM PROCEDURES

The Emergency Coordinator must notify company management when business operations can be transferred to the original facilities or to new facilities. As business operations are transferred back to normal operations, the recovery procedure will very quickly be phased down. The Emergency Action Operations Team must leave the Contingency Site with all property and materials belonging to the organization, and use due care and caution to protect all Company information.

The Emergency Coordinator and Readiness Team must maintain a full state of readiness during, and particularly after, returning to normal operations. The Emergency Action Operations Team will be directed to return materials back to their proper offsite storage, including current materials and media.

The Emergency Action Operations Team must inform all users that the emergency or disaster is over and that operations are now or soon to be returned to normal. The Emergency Control Center will be deactivated.

The final activity of the recovery process will be the meeting and debriefing of the Readiness Team, all Coordinators, and Emergency Action Team Leaders concerning the activities of the recovery. The Emergency Coordinator is responsible to make sure that events, problems and solutions, etc., are documented. Once documentation is complete, the Emergency Action Teams and Readiness Team can be deactivated. During the next review of the Plan, the Emergency Coordinator will be responsible to ensure that any lessons learned are incorporated into the Plan.

B. USER DEPARTMENT PROCEDURES

Upon notification from the Emergency Action Operations Team that the disaster is over, user departments will:

- Ensure that all materials have been collected from the disaster recovery work areas. This includes both traditional paper documents as well as electronically stored information.
- Resume operations at the repaired facility or new facility as appropriate. User departments shall follow their operations procedures to ensure a smooth transition in this process.

VI. After a Disaster

Following the disaster, each department will document the events that transpired including any recommended changes to their procedures. The disaster results will then be reviewed by F2OnSite management.

Appendix A – Distribution List

President

Chief Executive Officer

All Department Heads

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Business Continuity Business Resumption Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

BUSINESS CONTINUITY DISASTER RECOVERY PLAN

I. Purpose of the Business Continuity Disaster Recovery Plan

Information systems are an important resource for F2OnSite's (Company) employees. This Business Continuity Disaster Recovery Plan (hereinafter referred to as the "Plan") documents the strategies, personnel, resources, and procedures required to provide immediate response and subsequent recovery from emergencies and disasters including:

- Unplanned business interruptions
- Loss of critical services (computer processing, telecommunications)
- Loss of building access (contamination, etc.)
- Physical facility catastrophe (fire, sabotage, etc.)

II. Business Continuity Philosophy

The primary objective of business continuity is to help ensure the operation of F2OnSite's business by providing the ability to successfully continue operations in the event of a disaster or emergency.

Specific goals of the Plan relative to a disaster or emergency include:

- To detail the correct course of action to follow
- To minimize confusion, errors, and expense to the Company
- To effect a quick and complete recovery of services

Secondary objectives of the Plan are:

- To reduce risks of loss of services
- To provide ongoing protection of company assets
- To ensure the continued viability of this Plan

III. Policy Statement

Company management is responsible for protecting all assets of F2OnSite's organization. These assets include employees, physical property, information, and records relating to the conduct of the business.

Management personnel are specifically responsible for:

- Identifying and protecting all assets within assigned areas of control
- Ensuring that all employees understand their obligation to protect the organization's assets
- Implementing/observing security practices and procedures that are consistent with generally accepted practice and with the specific guidelines stated in this Plan.
- Noting any variance from established security practices and initiating corrective action
- Assigning responsibilities for establishing, maintaining, and coordinating F2OnSite's Information Systems Business Continuity Recovery Plan

IV. Overview of the Plan

The Plan is a comprehensive document containing the necessary instruction, policies, organization, and information required to be prepared for an emergency or disaster that would affect F2OnSite's information systems. The Plan consists of the following major sections:

- The Readiness Team. This section establishes personnel known as the Readiness Team. This team is responsible for constructing and maintaining this Plan, managing business continuity information systems activities, and for the continued viability of the Plan.
- Major Services, Users, and Key Considerations. This section describes the critical applications, identification of users, and key considerations such as equipment configurations, user work schedules, and processing priorities.
- General Procedures for Potential Interruptions. This section describes the service and general instructions for handling each type of interruption. Typical interruptions include fire, power outage, and telecommunications failure.
- Policies for Reducing Risks. This section includes policies designed to reduce risks of emergencies or disasters occurring, of excessive damage when they do occur, and of failing to recover from an emergency or disaster.
- Contingency Site. This section identifies the Contingency Site and describes the facilities provided.
- Procedures for an Emergency Or Disaster. This section describes the instructions and procedures to be followed in the event of an emergency or disaster.
- Maintenance Of The Plan. This section contains the policies and procedures needed to ensure that the Plan remains viable as the business environment evolves.

V. Example Recovery Scenarios

A. Three phases of recovery

The scenario for recovery following an emergency or disaster involves three "phases":

1. The initial response of the Readiness Team
2. Implementing recovery plans
3. Restoring normal operations

Although the three phases occur in every recovery situation, the tasks and the people involved vary according to the nature of the emergency or disaster and its severity.

Following are three example recovery scenarios for understanding the steps involved in recovering from an emergency or disaster. The three examples also illustrate some of the differences in recovery steps and elapsed times for minor, moderate, and major severity:

- Telecommunications failure affects several critical departments
- No commercial power available for five days
- Major fire destroys F2OnSite's offices and network server room

B. Example #1 - partial interruption of services (minor severity)

Scenario: Telecommunications equipment failure affects several critical departments

<u>RECOVERY SEQUENCE</u>	<u>Elapsed Time After Failure</u>
INTERRUPTION OF SERVICE	0 hour
RECOVERY PHASE 1	
Initial Response of Recovery Team:	
- Problem/repair alternatives evaluated	1 hour
- Interruption of service assessed	1.5 hours
- Decision to implement recovery actions	1.5 hours
RECOVERY PHASE 2	
Business Continuity Recovery Plans Implemented:	
- Affected users notified	1.5 hours
- PCs in less critical locations are temporarily assigned to the affected users (requires users to go to other departments)	2 hours
- Dialup arrangements implemented & tested	3 hours

(for use by a few critical functions)

- Work schedule adjusted for the delay 3 hours

RECOVERY PHASE 3

Normal Telecommunications Service Restored:

- Equipment repaired 24 hours
 - Affected users notified 24 hours
 - Normal telecommunications restored 25 hours

TOTAL RECOVERY TIME

25 hours

C. Example #2 - major failure but network intact (moderate severity)

Scenario: No commercial power available for five (5) days

<u>RECOVERY SEQUENCE</u>	<u>Elapsed Time After Failure</u>
INTERRUPTION OF SERVICE	0 hour
RECOVERY PHASE 1	
Initial Response of Recovery Team:	
- Problem/repair alternatives evaluated	1 hour
- Interruption of service assessed	1.5 hours
- Decision to implement recovery actions	1.5 hours
RECOVERY PHASE 2	
Business Continuity Recovery Plans Implemented:	
- Contingency site notified	2 hours
- Activate Emergency Control Center	3 hours
- Emergency Action Teams* notified and assembled (* only selected Emergency Action Teams activated)	3 hours
- Assemble backup tapes, supplies, other needed materials and documentation	3-5 hours
- Prepare recovery computer(s) for operation	8-24 hours
- Travel to & assemble at Contingency Site	12-48 hours
- Recover any lost work in progress	12-48 hours
- Resume information systems operations on recovery basis (probably reduced service levels)	12-48 hours

RECOVERY PHASE 3

Network Server Operations Restored:

- Problem resolved at original location	5 days
- Network servers tested	5 days
- Operations transferred back to primary offices	5-6 days
- Operations normalized	7 days

TOTAL RECOVERY TIME

7 days

D. EXAMPLE #3 – CENTRAL NETWORK AND OFFICES DESTROYED (MAJOR SEVERITY)

Scenario: Major fire destroys F2OnSite's offices and network server room

<u>RECOVERY SEQUENCE</u>	<u>Elapsed Time After Failure</u>
INTERRUPTION OF SERVICE	0 hour
RECOVERY PHASE 1	
Initial Response of Recovery Team:	
- Problem/repair alternatives evaluated	1 hour
- Interruption of service assessed	1.5 hours
- Decision to implement recovery actions	1.5 hours
RECOVERY PHASE 2	
Business Continuity Recovery Plans Implemented:	
- Contingency site notified	2 hours
- Activate Emergency Control Center	3 hours
- Emergency Action Teams* notified and assembled (* all Emergency Action Teams activated)	3 hours
- Assemble backup tapes, supplies, other needed materials and documentation	3-5 hours
- Prepare recovery systems for operation	8-24 hours
- Travel to & assemble at Contingency Site	12-48 hours
- Recover any lost work in progress	12-48 hours
- Resume computer service operations on recovery basis (probably reduced service levels)	12-48 hours
RECOVERY PHASE 3	
Replacement Network Server Room Operational:	
- New network server facilities established	3 weeks

- New hardware obtained and installed	3 weeks
- New network server tested and made operational	4 weeks
- Operations transferred to new server	4 weeks
- Operations normalized	6 weeks

TOTAL RECOVERY TIME **6 weeks**

VI. The Readiness Team

A. Purpose of the readiness team

The purpose of the Readiness Team is to establish and direct plans of action to be followed during an interruption or cessation of information systems caused by an emergency or disaster. As the name implies, the Readiness Team maintains readiness for emergencies and disasters by means of this Information Systems Business Continuity Recovery Plan. The Readiness Team is also responsible for managing recovery activities and can be thought of as the "recovery management team". Through the recovery plans, the Readiness Team provides for:

- The safety of personnel
- The protection of property
- The continuation of business

B. Organizing and planning

The Readiness Team consists of:

- Emergency Coordinator
- Alternate Emergency Coordinator
- Contingency Site Coordinator
- Emergency Action Team Leaders
- Any other designated individuals

The list of designated members of the Readiness Team, showing names and functions, is provided in Appendix A.

The responsibilities of individuals assigned to the Readiness Team are in addition to their regular assignments and are made on the basis of familiarity and competence in their respected areas of specialties.

This Plan is administered by the Emergency Coordinator and the Alternate Emergency Coordinator. The Alternate Emergency Coordinator is also responsible for maintaining an Emergency Control Center. Emergency Action Teams are used to facilitate the response to various types of emergency and disaster situations. A Contingency Site Coordinator and

Alternate are designated for emergencies and disasters requiring offsite operations at a Contingency Site.

The responsibilities and functions of the Coordinators, Emergency Action Teams, and the Emergency Control Center are discussed in the sub-sections below. Emergency Action Teams include:

- Emergency Action Operations Team
- Emergency Action Applications Team
- Emergency Action Hardware Team
- Emergency Action Facilities Team
- Emergency Action Administrative Assistance Team

See Section XI. Emergency Action Teams which specifically describes each type of Emergency Action Team.

C. Emergency coordinator

The Emergency Coordinator is responsible for developing and coordinating the Readiness Team. During an emergency or disaster situation, the Emergency Coordinator will activate and direct all activities until the situation is under control. In the absence of the Coordinator, the Alternate Emergency Coordinator will assume these duties. Additionally, the Emergency Coordinator is responsible for the following:

- Reviewing, evaluating, and updating this Plan at least annually to assure that all emergency and disaster situations have been adequately considered and that appropriate recovery plans and procedures have been prepared.
- Ensuring that the Emergency Readiness Team and other employees receive proper training of recovery plans and procedures. This will routinely be done as a part of annual (or more frequent) tests of the Plan. The Coordinator will also ensure that new employees are properly trained and that certain emergency and disaster procedures are reviewed as frequently as necessary.
- Conducting meetings with the Alternate Emergency Coordinator, the Contingency Site Coordinator, and the Emergency Action Teams as necessary.
- Keeping all members of the Emergency Readiness Team fully briefed on all aspects of the recovery process.
- Evaluating the readiness and proficiency of each Emergency Action Team and the appropriateness of their assignments.
- Keeping management informed of the status of the Emergency Readiness Team and the recovery.
- Communicating the status of emergency and disaster situations to management promptly and efficiently.

- Maintaining liaison with local fire and police agencies, other company locations, and other involved parties as appropriate.

The designated Emergency Coordinator is identified in Appendix A.

D. Alternate emergency coordinator

In the absence of the Emergency Coordinator, the Alternate Emergency Coordinator will assume the duties of the Emergency Coordinator. The following additional duties are assigned to the Alternate Emergency Coordinator:

- Assisting the Emergency Coordinator in maintaining an up-to-date Plan, emergency and disaster procedures, and in directing proper distribution of the Plan.
- Providing emergency evacuation programs and posting them on bulletin boards or otherwise distributing them to all personnel.
- Maintaining up-to-date contact information for Offsite Emergency Coordinator, Emergency Action Team members, emergency telephone numbers, and vendors.
- Activating the Emergency Control Center and administering the Control Center itself during an emergency or disaster situation.
- Keeping the Emergency Control Center properly equipped and in a state of readiness.
- Monitoring all tests of the Plan, and recording the progress, problems, and successes.

The designated Alternate Emergency Coordinator is identified in Appendix A.

E. Contingency site coordinator

The Contingency Site Coordinator is responsible in helping to establish and maintain written procedures to be followed during emergency or disaster situations requiring operation at a Contingency Site. During such an emergency or disaster, the Contingency Site Coordinator will direct operations at the Contingency Site and communicate with the primary location via the Emergency Control Center. In the absence of the Contingency Site Coordinator, the Alternate Emergency Coordinator will assume the duties of the Contingency Site Coordinator.

In addition, the Contingency Site Coordinator is responsible for the following:

- Periodically reviewing and evaluating the Plan to assure the Contingency Site has been adequately prepared.
- Assuring that the Contingency Site meets the minimum requirements for testing and recovery purposes.

- Overseeing periodic tests at the Contingency Site and maintaining technical readiness for operation of services from the site.
- Recommending to the Emergency Coordinator any necessary changes or improvements in the Plan.
- Keeping the Emergency Coordinator informed of the status of the Contingency Site and any changes relative to requirements or planning.
- During emergency or disaster offsite operations, communicating the status of operations via the Emergency Control Center.
- Assuming responsibilities of the Emergency Coordinator in the event that both the designated Emergency Coordinator and the Alternate Coordinator are unavailable for duty.

The designated Contingency Site Coordinator is identified in Appendix A.

F. Use of emergency action teams

Emergency Action Teams are used for specific functions during an emergency or disaster situation and subsequent recovery. The teams and their responsibilities are defined in Section XI Emergency Action Teams. Members of Emergency Action Teams are identified in Appendix A.

In general, the Team Leader of each Emergency Action Team is responsible for the following duties:

- Periodically reviewing and evaluating the emergency and disaster planning with particular emphasis on completeness and accuracy of specific recovery procedures.
- Each Emergency Action Team's responsibilities, assignments of and changes in personnel, and availability of equipment, facilities, and services.
- Recommending to the Emergency Coordinator any necessary changes or improvements in the Plan.
- Recruiting and training personnel for emergencies and maintaining proficiency at a high level. All Emergency Action Team members must be capable of performing their duties quickly under stress.
- Informing the Emergency Coordinator of any additions or changes of individuals assigned to an Emergency Action Team.

G. Emergency control center

In an emergency or disaster, the Emergency Control Center will be established from which all communications and activities will be directed. The Emergency Control Center will be used to coordinate the management of recovery procedures, and will serve as the center of all communications between the Emergency Coordinators, the Emergency Action Teams, and all

other personnel. The administration of the Emergency Control Center is the responsibility of the Alternate Emergency Coordinator.

The designated Emergency Control Center and alternate locations are identified in Appendix B. The Emergency Control Center is activated when an emergency or disaster has occurred, particularly when the personal safety of employees or property is jeopardized. Readiness and activating of the Emergency Control Center are the responsibility of the Alternate Coordinator. Directing activities and communications from the Emergency Control Center is the responsibility of the Emergency Coordinator.

The Emergency Control Center provides centralized and coordinated control of communications during emergencies and disasters. When the Emergency Control Center is in operation, Emergency Coordinators and Action Team Leaders will coordinate with the Emergency Control Center and keep it informed of status and progress.

If conditions warrant closing of facilities, the Emergency Control Center will communicate the closing notice through the management chain to all employees.

VII. Major Services, Users, and Key Considerations

A. Purpose of major services, users, and key considerations

It is necessary to the well being of Company that critical applications processed on internal (in-house) and external (outsourced) information systems be kept in service even in the event of an emergency or disaster. Critical applications include:

- Accounting (internal)
- E-mail (internal)
- Internet access (external)
- BAS
- Phones
- Active Directory

Each critical application processed internally and externally is described here in terms of the key considerations in a recovery scenario.

B. INTERNAL SERVICES AND APPLICATIONS

The following services are processed on internal information systems:

Department	Representative(s)	Process	Time when issue becomes High priority

Accounting/Finance	XXXXXX	Accounts Payable Lack of info for decisions	1 week 2 weeks
Production	XXXXXX	Process Paid once per week	3 days
Customer Service	XXXXXX	Inbound call center phones	4 hours
Human Resources	XXXXXX	Payroll on processing day Benefits	2 hours 3 days
Sales	XXXXXX	Receipt of RFP via email Claims inquiries	1 day 1 week

Software applications processed on internal systems include:

Application Software	Server Name	Databases used	Full backup	Stored Off-site	Recovery time	IT Priority
Active Directory	XXXXXX		Yes	Yes	4 hr	High
Internal Domain Name Server	XXXXXX		Yes	Yes	4 hr	High
External Domain Name Server	XXXXXX		Yes	No	4 hr	High
Exchange Mail Server	XXXXXX	Exchange	Yes	Yes	4 hr	High
Production application	XXXXXX	XXXXXX	Yes	Yes	8 – 12 hr	High
Web Server	XXXXXX	XXXXXX	Yes	No	6 hr	High
Backup Server	XXXXXX		Yes	Yes	6 hr	Medium
File Server	XXXXXX		Yes	Yes	12 – 24 hr	Medium
Print Server	XXXXXX		Yes	Yes	4 hr	Medium
Fax Server	XXXXXX		Yes	Yes	8 hr	Medium
VPN Server	XXXXXX		No	No	4 hr	Low
Accounting	XXXXXX	Yes (many)	Yes	Yes	8 hr	Low
Voicemail Server	XXXXXX		Yes	No	12 – 24 hr	Low

C. External services and applications

Third party service providers include:

Vendor	Service provided	IT Priority
Vendor	Internet and Phone Service Provider	High
Vendor	Tape backup off-site storage	High
Vendor	Accounting system support	Medium
Vendor	Voicemail System Support	Low

Service provider	Importance (high, med, low)	Recovery time objective	Recovery point objective
Provider 1	High	1 day	N/A
Provider 2	High	3 days	3 days
Provider 3	Low	1 week	N/A
Provider 4	High	3 days	N/A
Provider 5	High	1 week	1 week

D. Information systems equipment considerations

Application software runs on an internal network server computer with numerous PCs and printers directly connected to F2OnSite's network. In recovery situations, the minimum equipment configuration is identified in Appendix E.

E. Special considerations

The following special equipment considerations are necessary components to a successful recovery effort. Each employee is assumed to require:

- Desk
- Computer
- Phone
- Printer
- Internet access
- Email access

User department work area requirements include:

Department	Minimal staff required	Other resources required
Accounting/Finance	XX	Checks stored off-site
Production	XX	
Customer Service	XX	Fax, copier
Human Resources	XX	Facilities for staff
Sales	XX	

VIII. General Procedures for Potential Interruptions

A. Purpose of general procedures for potential interruptions

This section includes a series of recovery plans that identifies prompt and appropriate actions to take in potential emergencies, disasters, or events causing interruption of information systems. Training sessions are to be held periodically to familiarize employees with these procedures and to outline responsibilities in the event of such emergencies. *The Emergency Coordinator will arrange these training sessions.*

Copies of this Plan must be kept in key locations for ready reference. Members of the Readiness Team must be given copies of this Plan. The Distribution List is contained in Appendix F.

Assets of the Company are extremely important to its very existence. The most important asset is F2OnSite's personnel. Risks must not be taken to save other assets where personnel may be in jeopardy.

B. Recovery plan for fires

Preventing Fires

- Periodically, review all areas of responsibility for combustible materials.
- Check operational areas before employees leave each day.
- Educate the staff, and new employees, about the fire plan. All employees must have periodic reviews of the fire plan on a schedule to be determined by Company management.
- Regular site inspections which include general area review, and checks of electrical connections, fire extinguishers, and smoke detectors must be made every 12 months by The Alternate Emergency Coordinator.

- Smoking is only allowed in areas designated by Company management. Other areas involving quantities of combustible materials must be reviewed and posted for NO SMOKING, if necessary.

Detecting Fires

F2OnSite's offices have a fire detection and suppression system. Smoke detectors are located in/on the ceiling. If smoke is detected, horns will sound and emergency evacuation should begin.

Extinguishing Fires

- Company management will arrange employee fire extinguisher training. The Alternate Emergency Coordinator must arrange to have all extinguishers inspected annually.
- An employee should only attempt to extinguish a fire if it is very small or confined to a particular piece of equipment. Otherwise, the fire department should be called by the receptionist and the building should be evacuated immediately.
- DO NOT PLAY HERO. If the fire is of any consequence, leave the building immediately.

Evacuating If Fire

- If the fire is such that employees must evacuate the building, a member of the Emergency Action Operations Team should notify the receptionist to call 911 to contact the fire department.
- Employees should not take backup media with them when they evacuate the building. A member of the Emergency Action Operations Team stores backup media offsite on a rotating basis.
- Before evacuation, a member of the Emergency Action Operations Team must shut off all power to equipment and overhead lights. If there is time, Emergency Action Operations Team employees should power down system(s) before cutting power.

Goals

- Protect the lives and health of employees
- Protect essential documents, records, and data
- Minimize damage to data processing equipment and other property

Procedures for Fires

- A member of the Emergency Action Operations Team should notify the receptionist to call 911 and contact the fire department immediately. Give the following information:
 - Your Name
 - Your Department and location
 - Nature of Emergency

- The receptionist will provide 911 with the building address, the location of the fire, and type of fire it is (paper, electrical, etc.).
- If time permits, a member of the Emergency Action Operations Team will shut down systems
- A member of the Emergency Action Operations Team will cut off all electrical power
- If the fire is small, use a fire extinguisher after you have notified the receptionist to call 911. Pull the pin on the fire extinguisher, then discharge the extinguisher by aiming at the base of the fire using a side-to-side sweeping motion.

C. Recovery Plan For Electrical Outages

An electrical outage is most likely caused by a failure of the public electricity utility. In most cases, return of electricity is usually within a few hours, but the Emergency Coordinator is responsible to contact the electricity company to determine how long the outage is expected to last.

Ordinarily, it is necessary to wait until electricity is restored with the possibility that repairs to data files will be necessary. In the unlikely event that electricity cannot be restored for days, then the Emergency Coordinator will contact Company management and coordinate electricity with the Emergency Action Facilities Team.

Procedures For Electrical Outages - If an electrical problem exists, even though public power is not out of service, such as after restoring electricity, the following need to be notified by the Emergency Action Facilities Team:

- Emergency Coordinator
- Electricity Company

D. Recovery plan for telecommunications failures

Failures of the computer telecommunications system fall into two basic categories:

- Hardware Failure - When a piece of telecommunications equipment fails, it must either be repaired or replaced, like any other hardware failure. Faulty or damaged equipment will be replaced as needed.
- Line Failure - The line is a utility service provided by a communications carrier company. If a line fails, just as in an electrical outage, F2OnSite is dependent on the utility to fix the problem and restore service. However, if the entire phone system is down in the area, recovery plans must be considered if the outage is predicted to be of long duration. If the outage is predicted to last so long as to affect business operations seriously, the Emergency Coordinator must consider switching operation to F2OnSite's Contingency Site.

An extreme phone system outage will affect the entire business operation, in which case the Contingency Site is one option for temporarily operating the business or some key portions of

the business until repairs are made. See Section X Contingency Site for specific site information.

Procedures For Telecommunications Failures

- Obtain replacement equipment if Company experiences a telecommunications hardware failure
- Notify telecommunications provider a line failure occurred and the circuit is down
- Use dial-up lines at main office or high speed line at Contingency Site

E. Recovery plan for flooding

Preventing Floods - The facility design must be reviewed at least annually by the Alternate Emergency Coordinator for knowledge of risks relative to flooding. The Alternate Emergency Coordinator must know where water pipes and drains are in respect to information systems equipment. If possible, route pipes and add drains to reduce the risk of flooding. Know what the potential is for flooding from above (upper floors or roof).

The Alternate Emergency Coordinator must know how the server room facility lies physically in respect to external floods coming in and what steps to take to prevent flooding. If the opportunity arises to choose a new server room, Company management should take into account the flood plain and building construction.

During heavy weather conditions, particularly rain, the Alternate Emergency Coordinator will inspect windows and roofs in proximity to the server room for flooding or water buildup. The Alternate Emergency Coordinator, or contract maintenance staff, must inspect at least twice annually all pipes and valves in proximity to the server room for leaks.

Detecting Floods - The detection of water within the server room is vitally important to prevent electrical shocks, short-circuits, or equipment damage.

Evacuating If Floods

- If flooding is such that employees must evacuate the building, the Emergency Action Operations Team should notify the receptionist to contact the Emergency Action Facilities Team.
- It is not necessary to take backup media with you when evacuating the building. All systems are backed up offsite on a frequent enough basis to make recovery possible from tapes stored at the offsite storage location.
- Before evacuating, all power must be shut off to equipment and overhead lights. If there is time, the Emergency Action Operations Team should power down system(s) before cutting power.

Goals

- Protect the lives and health of employees
- Protect essential documents, records, and data
- Minimize damage to data processing equipment and other property

Procedures for Flooding

- A member of the Emergency Action Operations Team should notify the receptionist to call the Emergency Action Facilities Team immediately. Give the following information:
 - Your Name
 - Your Department and location
 - Nature of Emergency
- The receptionist will provide the building address and the location and type (pipe, roof, etc.) of flooding.
- If flooding is such that there is no risk of electrical shock (i.e. the flooding has just started), a member of the Emergency Action Operations Team must power down the system(s) before cutting power.
- If time allows, the Emergency Action Operations Team must do all that is possible to protect the equipment. If flooding is coming from overhead, the Emergency Action Operations Team must drape the equipment with heavy plastic.
- If flooding is such that employees should evacuate the building, the receptionist must notify Company management immediately.

F. Recovery plan for hardware failures

Appendix E provides a list of information systems equipment used by Company. In most circumstances, the hardware can be repaired to restore operation within a short period of time. Even if the downtime were as long as a day, the preferred approach is to allow the engineers to make their repairs in the normal manner.

Hardware failures generally require either repair or replacement. Specific recovery plans are outlined below.

Network Servers - In the event that a network server is out of service for an extended period of time, such that Company will be seriously affected, the Emergency Coordinator will coordinate with appropriate vendors to correct or replace.

Peripherals And Other Equipment - Peripherals are devices that are attached externally to network servers (e.g. printers, scanners, external tape drives, etc.). Other devices, such as Fax machines and copiers may not be connected to the network but are needed for other functions. Should a hardware failure be prolonged for an extended period of time, the operation of the dependent user department will be seriously affected.

Procedures For Hardware Failures - Appendix C provides a complete list of network server and peripheral vendors. These vendors can assist in determining loaner equipment availability as well as timeframe to obtain replacement parts and/or new equipment.

G. Recovery plan for software failures

Desktop, operating system, and other systems software may encounter errors that result in system downtime. Equipment vendors and software manufacturers can assist in restoring systems to normal functionality. Software manufacturers frequently provide bug fixes and software patches for known problems. Appendix C provides a list of software vendors.

The Contingency Site Coordinator approves the installing of changes provided by software manufacturers. Should changes cause a serious failure of network services, the Contingency Site Coordinator will take the appropriate action to correct the problem either by authorizing a manufacturer-provided "fix" or by designating that the system software be returned to the version prior to loading the changes.

It is very unlikely that system software could cause a major service failure. However, in such an event, the Contingency Site Coordinator will oversee restoring the software from the appropriate backup.

Applications Failures - Some of F2OnSite's applications packages were acquired from third-party sources and are maintained by those companies. These vendors can assist in correcting application problems. Appendix C provides a list of application software vendors.

Applications software is very similar to systems software concerning failures of new versions of the programs. In-house change control procedures must be developed to provide for adequate testing before making changes and for backing out the changes if problems are detected.

However, a more serious type of application failure is one where, through error of a program, a user, a maintenance programmer or by other means, data is caused to be incorrect to the degree that business consequences are serious.

In this case, the staff that supports the failed application must determine how the erroneous data will be corrected. Backups of data files may or may not be useful depending on the amount of time elapsed during which the error proliferated. In serious cases, special-purpose programming may be required to repair the data. In the worst case, the original source transactions will be re-input to recreate the data files.

IX. Policies For Reducing Risks

A. Protecting data

Information systems data is protected by combining backup and offsite storage procedures. Backups copy the data from disk to removable media (usually magnetic tape) so that data that is lost or damaged for any reason can be restored. Offsite storage for magnetic tapes (or other forms of information) protects the data if the information system itself is destroyed. No business is likely to survive if its vital records are destroyed. Recovery is possible when an information system is destroyed but the data is protected at another location.

B. Backup procedures

The backup procedures for information systems data are as follows:

- Full backups of critical data are completed on a daily basis
- Once a week (Fridays), backups rotated offsite
- Special backups for legal records purposes should be performed as required, usually once each year (January).

C. Backup storage procedures

Backup tapes are stored both on-site and offsite. On-site storage consists of tapes located in the media safe in the IT office. The offsite storage facility for network recovery is fully identified (name, location, etc.) in Appendix B.

The backup storage procedures are as follows:

- Nightly backups stored on-site through a weekly rotation
- Weekly full backups stored offsite after they are on-site for a week
- Full backups kept with a rotation
- Special backups, including legal records archives, should be kept offsite for a period of seven to ten years, depending on the contents and purpose of the backup

D. Protecting network servers

Procedures for protecting F2OnSite's network servers:

- Physical security. The computer room remains locked at all times and only the Emergency Coordinator, Alternate Emergency Coordinator and Company management have keys.
- Electronic component damage. Damage due to electrical spikes, surges, over-voltages, and under-voltages reduced by an uninterruptible power supply (UPS) system with power surge protection.
- Security. Strictly adhering to F2OnSite's "Policies and Guidelines On The Use of Information Systems" and "Policies and Guidelines To Secure Information Systems" document procedures protect F2OnSite's information systems.

E. Protecting vital records

Many documents and records are vital to the operation of Company. Company has implemented procedures and plans to protect these vital records. Vital records (checks, invoices, journal entries, etc.) may be required in order to recreate lost electronic data.

Company management specifies how long records must be retained for practical and legal requirements. The schedule is reviewed by the Emergency Coordinator to ensure aspects of the Plan adhere to F2OnSite's retention schedule.

Many vital records are backed up by the network server data backup procedures. Other records, if destroyed, could be replaced by contacting vendors or other sources. Appendix C provides a list of vendor contacts.

F. Backup of data, hardware, supplies & documentation

All data, spare hardware, supplies, and documents identified as critical for F2OnSite's recovery process, are stored in offsite storage. The offsite storage location is identified in Appendix B.

Backups stored offsite include:

- Computer data and software. All data resident on the network server(s), including systems software and applications software, are backed up on a routine basis. The Contingency Site Coordinator is responsible for observing backup procedures at the Contingency Site.
- Critical spare hardware items. A Contingency Site can be used in the event the primary network server is no longer operational. See Section X Contingency Sites. Planning for special peripheral and telecommunications equipment is described in Appendix E. The Alternate Emergency Coordinator is responsible for reviewing backup procedures. Additional equipment such as PCs, printers, Fax machines, copiers, etc. are readily available and are not backed-up at an offsite location.
- Critical operating supplies. Critical supplies, including special forms and items for the Emergency Control Center, are stored in offsite storage. If Contingency Site operations are required, enough supplies will be available to continue operations until more supplies can be obtained from F2OnSite's vendors. The Alternate Emergency Coordinator is responsible for backing up operating supplies offsite.
- All critical documentation. Critical documentation is backed up offsite to assist recovery. Documents that should be maintained in offsite storage include this Plan, system startup and shut down procedures, and a copy of the relevant passwords.

G. Insurance

All property of the Company, including information systems equipment, is insured under F2OnSite's insurance program. This policy insures the replacement value of the property

against most natural kinds of damage or destruction, but does not cover the cost of lost business or replacing lost records.

The information systems equipment is not separately scheduled, but the total coverage must be sufficient to cover the equipment even if it were totally destroyed along with the other property of the organization. The Emergency Coordinator is responsible for informing Company management of the acquisition of new equipment and its value, and to verify annually the accuracy of the information.

X. Contingency Site Description

A. Emergencies and disasters

An emergency or disaster may require activation of the Contingency Site if information systems are unable to operate. Reasons may vary from actual destruction of the server room to less severe circumstances that affect information systems while leaving the server room intact.

If necessary, equipment will be replaced by the appropriate vendors on a time and materials basis. No prior approval is needed to purchase the replacement equipment. Follow the normal Company policy regarding accepting vendor equipment approving invoices. In the event equipment needs to be replaced, start the process by placing a telephone call to the appropriate vendor(s). Appendix C contains a list of vendor contacts.

B. Contingency site space and resource requirements

The Contingency Site contains office and server room space and related resources as identified below:

- Total person capacity
- Emergency Action Operations Team support staff
- PCs
- Printers
- Fax machines
- Telephone lines
- Internet connectivity
- Security features: lockable cabinets for sensitive documents/forms
- Facilities: locks on doors
- 24 hour access to Contingency Site

C. Recovery plan testing

The Emergency Coordinator schedules tests of the Contingency Site. Tests must observe the following schedule restrictions:

- Tests must be coordinated with the Contingency site – recommended annually

- Actual emergency situations take precedence over tests
- User departments are limited to 6 hours of test time each day
- Emergency Action Operations Team is allocated 6 hours of processing, backup, and administrative time each day

XI. Emergency Action Teams

A. Responsibilities of the emergency action teams

The following Emergency Action Teams have been defined for use in disasters or major emergencies. The purpose, responsibilities, and members of these Teams are described on the following pages. The Teams will be activated selectively by the Emergency Coordinator and/or the Readiness Team according to the nature of the emergency. The Teams report to the Emergency Coordinator, or the Contingency Site Coordinator if offsite.

Emergency Action Teams:

- Emergency Action Operations Team
- Emergency Action Applications Team
- Emergency Action Hardware Team
- Emergency Action Facilities Team
- Administrative Assistance Team

The use of Emergency Action Teams and the general responsibilities of Team Leaders are discussed in Section IV The Readiness Team. Designated Team Leaders and members of each Emergency Action Team are identified in Appendix A.

B. Emergency action operations team

The purpose of the Emergency Action Operations Team is to ensure resuming of information systems and related processing following an emergency or disaster. The Emergency Action Operations Team oversees processing at the Contingency Site until such time that operations can resume at the original or replacement network server room.

Responsibilities Of The Emergency Action Operations Team

- Periodically review and evaluate the appropriateness and completeness of procedures for backups, offsite storage, and recovery. Backups must include data, software, forms and other supplies, and operations documentation.
- In an emergency or disaster, obtain all appropriate backups from offsite storage, including tapes, supplies, and documentation.
- Participate in initiating operations at the Contingency Site. Then continue recovery operations until the Contingency Site is no longer required. This will require

communication with the other Teams to understand levels of service and functional differences in the recovery mode, with the user departments to prepare a revised processing schedule, and with the Offsite or Emergency Coordinators concerning status of work.

- Coordinate with users on how to submit input to and receive output from the Contingency Site.
- If recovery operations continue for an extended period of time, ensure that adequate levels of operating supplies are maintained at the Contingency Site.
- Provide manpower to support the offsite operations. Coordinate with the Emergency Action Administrative Assistance Team for transportation and housing of the Emergency Action Operations Team staff. Revise schedules as appropriate to the needs of the emergency situation.

C. Emergency action applications team

The purpose of the Emergency Action Applications Team is to ensure proper functioning of the applications at the Contingency Site. The Emergency Action Applications Team also coordinates with users on how applications should be operated during the recovery period.

Responsibilities Of The Emergency Action Applications Team

- The Emergency Action Applications Team must participate in preparing and conducting tests at the Contingency Site. If a problem exists on how an application will operate at the Contingency Site, the Emergency Action Applications Team must prepare and document solutions for the problem. Applications documentation and a copy of Plan should be stored offsite.
- In an emergency or disaster, obtain offsite documentation and a copy of Plan from the Emergency Action Operations Team in order to assist in restoring Contingency Site operations.
- Coordinate with the Emergency Action Operations Team and users to determine work that was in progress at the time of the disaster. When operations are restored at the Contingency Site, the Emergency Action Applications Team must first help recover any lost work that was in progress.
- Once user work has been recovered, coordinate with the users about any changes in the way they will interface to their applications and provide assistance as necessary.

D. Emergency action hardware team

The Emergency Action Hardware Team is responsible for repair or replacement of computer hardware, installing and testing computer hardware, and all hardware planning - whether at the original site, the replacement site, or the Contingency Site.

Unless a separate Emergency Action Team is established, the Emergency Action Hardware Team is also responsible for telecommunications.

Responsibilities Of The Emergency Action Hardware Team

- Participate in evaluating and selecting F2OnSite's Contingency Site(s), testing at the Contingency Site, and all hardware-related planning.
- In an emergency or disaster, assess the extent of damage or the affect of failures on hardware and telecommunications.
- Coordinate with vendors in obtaining necessary repairs or replacement of hardware. Agreements should be negotiated in advance wherever possible for rush delivery of equipment or telecommunications facilities.
- Coordinate with purchasing, finance, insurance, and other departments in equipment salvage, insurance claims, and financing for replacement equipment.
- Install and test all new/replacement hardware or data lines, and supervise all problem solving.

E. Emergency action facilities team

The purpose of the Emergency Action Facilities Team is to restore or replace the server room and other information systems facilities following an emergency or disaster.

Responsibilities Of The Emergency Action Facilities Team

- Maintain current configurations of the information systems facilities. The configurations should include space layouts, lists of all facilities, such as air conditioning, power distribution, power conditioning, etc., and specify model numbers, capacities, electrical requirements, etc.
- In an emergency or disaster, assess the damage and recoverability of the facilities. If the facility is usable, proceed to organize immediate repairs.
- If the facilities are destroyed and not usable, locate replacement facilities that can be acquired quickly and are usable for a reasonably long period, if not permanently. Facilities include not only requisite square footage in a building, but also cabling, air conditioning, power, etc.
- Coordinate with facilities vendors the build out, equipment, installation, and permits. If possible, negotiate facilities space in advance.
- Coordinate with purchasing, finance, insurance, legal and other departments in ordering new equipment, contracting for space and build out, insurance claims, and financing new facilities.

F. Emergency action administrative assistance team

The Emergency Action Administrative Assistance Team is responsible for all activities in the recovery process that are not handled by other Emergency Action Teams. These activities

include arranging transportation, housing, shipping, etc., and performing clerical and other administrative functions.

Responsibilities Of The Emergency Action Administrative Assistance Team

- Develop and review administrative procedures of the Plan
- Participate in tests of the Plan to actually perform the administrative functions and evaluate procedures and requirements
- Handle all administrative arrangements for transporting, housing, shipping, expense advances, etc.
- Assist in facilitating arrangements and administrative approvals with other departments.
- Perform clerical and administrative functions as needed during the recovery

XII. Procedures for an Emergency or Disaster

A. Notifying the readiness team

The following recovery steps are for use in an emergency or disaster of a serious enough magnitude to require computer processing to be moved to a Contingency Site. A critical aspect of recovery is the quick reaction of the Emergency Readiness Team. The Readiness Team must notify appropriate personnel so that recovery can initiate as quickly as possible.

The Emergency Coordinator has established and will maintain the Emergency Notification List and will ensure that all key personnel have it available. The Emergency Notification List is contained in Appendix A.

In the event of an emergency or disaster, the following notifying procedures must be followed:

- The Emergency Coordinator should initiate the notification process as soon as possible. If no operations personnel are on duty, a security guard has been provided with the proper procedures and must notify the Emergency Coordinator who will then initiate the notification process.
- The Emergency Coordinator is at the top of the Emergency Notification List. If the Emergency Coordinator cannot be reached, the Alternate Emergency Coordinator must be contacted.
- The first member of the Readiness Team notified is responsible to notify other members of the Readiness Team and to initiate action. The initial action will be to assemble the Readiness Team at the Emergency Control Center or the Alternate Emergency Control Center.

B. Initial readiness team procedures

Once the Readiness Team has been notified, they must proceed to make an immediate assessment of the situation and to initiate appropriate actions.

Readiness Team Procedures

- The first member of the Readiness Team notified is responsible for notifying other members of the Readiness Team and to initiate action. The initial action should be to assemble the team at the Emergency Control Center or the Alternate Emergency Control Center.

If the Emergency Coordinator has not yet been reached, the Alternate or persons listed next on the Emergency Notification List will assume full responsibilities of the Emergency Coordinator, until he or she has arrived and

- been fully briefed. The Emergency Coordinator or Alternate Emergency Coordinator will implement the recovery plans.
- The Emergency Coordinator will make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.
- Based on the Readiness Team's assessment of the situation, the Emergency Coordinator will determine the severity of the problem and decide on the appropriate action.
- If the Readiness Team judges the emergency to be a major disaster, members of the Readiness Team, as directed by the Emergency Coordinator, must do the following:
 - Activate the Emergency Control Center
 - Notify the appropriate Emergency Action Teams
 - Notify Company management
 - Notify the offsite storage site
 - Notify the Contingency Site
- The appropriate correction or recovery plans will be implemented according to the severity of the emergency or disaster.

C. Activating the emergency control center

In the event of an emergency or disaster, a centralized control center will be established from which all communications and activities will be directed by the Emergency Coordinator. In the event that an alternate location becomes necessary, the Alternate Emergency Control Center will be used. The locations of the Emergency Control Center and Alternate Emergency Control Center are identified in Appendix B.

Emergency Control Center Procedures

- The Alternate Emergency Coordinator maintains an Emergency Control Center in a state of readiness. The Emergency Control Center is equipped with table(s), chairs and a telephone. If necessary, certain emergency supplies are backed up offsite along with other emergency materials.
- When the Emergency Coordinator has declared a major emergency, the Alternate Emergency Coordinator will proceed to take all steps necessary to activate the Emergency Control Center.

The Emergency Coordinator selects either the primary or Alternate Emergency Control Center. For either site, Company management has requisite keys and other items, including names, addresses, and phone numbers, necessary to gain access to the site(s).

- If necessary, telephones will be ordered from the telephone company for emergency installation, and supplies obtained from backup or other sources to properly equip the Emergency Control Center.
- The Emergency Coordinator will notify the Readiness Team of the location and telephone numbers of the Emergency Control Center.

D. Notifying action teams and company management

In the event of an emergency or disaster, the Emergency Coordinator must notify the Emergency Action Teams and Company management of the incident. Company management needs to know about the emergency and the current status of personnel, property, etc. The Action Teams are intended to carry out very specialized functions in a recovery situation, and will be called in to act according to the incident.

Procedures For Notifying Action Teams And Company Management

- The Emergency Coordinator must determine which Emergency Action Teams should be activated.
- The Emergency Coordinator must notify Company management and if the presence of Company management is required to support the emergency activities or recovery procedures.
- The Emergency Coordinator or his or her Readiness Team designate must notify the Emergency Action Teams.
- Company management, names, positions, phone numbers, and addresses are contained in Appendix A. Appendix A identifies management succession if managers are absent or unavailable. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. The Emergency Coordinator should inform the executives whether their presence is required and when.
- In activating the Emergency Action Teams, the Team Leaders of each required team will be called from the Notification List in Appendix A. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. Each Team Leader has a copy of the Plan and must initiate action appropriate to his/her Team. He or she is responsible for notifying the team to assemble and act according to their recovery plans.

E. Notification of offsite storage and contingency sites

Activation of recovery plans will require retrieval of backups, documentation, and supplies from offsite storage as well as establishing operations at the Contingency Site. Specific Emergency Action Teams, according to procedures identified in this Plan, will carry out these tasks. To

expedite the initial recovery process, the Readiness Team will notify both the offsite storage site that a disaster has occurred and that the recovery plans have been activated.

Notifying Procedures For Offsite Storage and Contingency Sites

- Notify the appropriate personnel that offsite storage materials will be required to recover from a disaster. The standing recovery procedures identify what items, (e.g. backup media, supplies, etc.) are to be removed from storage. The procedures also specify precisely what is to be done with the items. The offsite storage location is listed in Appendix B.
- Notify the Contingency Site that a disaster has occurred that requires activation of recovery operations. The Contingency Site is listed in Appendix B.

F. Summary of procedures for recovery operations

This section provides an overview of recovery operations. Summary Of Procedures:

- The Emergency Action Operations Team, or designated members, will go to the offsite storage site and remove the items required by the recovery plans. Because of separate notification by the Readiness Team, the materials are expected to be gathered and ready by their arrival. The Emergency Action Operations Team will verify the materials, making any necessary adjustments, and then assemble at the Emergency Control Center.
- All other activated teams will assemble at the Emergency Control Center for briefing, discussion of any identified problems, and coordination of the recovery plans.
- The Emergency Action Applications Team will proceed to identify the work in progress that needs to be recovered and how that can best be accomplished. They will be responsible for notifying the user departments and coordinating their interface procedures.
- The Emergency Action Operations Team will proceed to the Contingency Site immediately and begin loading software and data to prepare for computer operations. Once established, processing will be maintained at the Contingency Site as long as required.
- If hardware has been destroyed, damaged, or negatively affected, the Emergency Action Hardware Team will proceed to take the appropriate recovery measures to repair or replace the affected hardware.
- If facilities have been destroyed, damaged, or negatively affected, the Emergency Action Facilities Team will proceed to take the appropriate recovery measures to repair or replace the affected facilities.
- The Emergency Coordinator will continue to maintain the Emergency Control Center as long as appropriate, and will coordinate the recovery operations until they can be returned to a normal, non-emergency state.

G. Initial procedures at contingency site

Contingency Site personnel will take the necessary initial steps following our notification that Company has had an emergency and will be using their systems. These procedures include preparations, both general (for them) and unique to our technical system requirements, which they can or need to accomplish before our arrival at their site.

H. Initial procedures at offsite storage site

The following procedures are to be performed by the offsite storage site as the initial steps following our notification that we have had an emergency and require materials from offsite storage.

Procedures At Offsite Storage

- Take the following materials from storage to a staging area for pick up:
 - The most recent backup media
 - All backup supplies
 - All backup documentation
 - Vendor supplied documentation can be supplied at a later date (if needed)
- DO NOT deliver the materials unless specifically requested. The procedure calls for the Emergency Action Operations Team to go to the storage site, verify that the correct backup materials are being taken, and take the materials with them to the Emergency Control Center. Some materials may be left at the Control Center and some will be taken to the Contingency Site.

I. Pickup of backup materials by emergency action operations team

The following procedures concern the picking up of materials stored offsite.

Procedures For Pickup Of Backup Materials - The Emergency Action Operations Team Leader should arrange for up to two members of the Emergency Action Operations Team to proceed directly to the offsite storage site to pick up all necessary backup materials in one trip. The Emergency Action Operations Team Leader will know from tests or reviews of items in storage how much vehicle capacity is needed. Team members with the appropriate type and size of vehicles (for transportation and protection of materials) will be specified to pick up the materials.

At the storage site, the team members will review the materials for correctness and appropriateness to the requirements of the emergency. See standard emergency items specified in this Plan and the complete list of items backed up in offsite storage. If there are problems identified with selected materials, the team members will attempt to select the correct items before dividing the materials into two groups. The materials should be grouped according to destination – Emergency Control Center or Contingency Site - before removal to their vehicles.

Contingency site materials include:

- The backup media
- Supplies
- One set of all documentation

Control Center materials include:

- Supplies for the Emergency Control Center
- Remaining documentation

The team members will proceed to take the materials to the Emergency Control Center. There the Contingency Site materials can be left in the vehicles (locked) and the other materials should be taken in to the Emergency Control Center.

J. Assembling and coordinating of all emergency teams

These procedures address the initial meeting of the Emergency Action Teams with the Emergency Coordinator and other members of the Readiness Team.

Assembling and Coordinating Procedures

- When all the required Action Teams have been assembled at the Emergency Control Center, the Emergency Coordinator will brief the Action Teams on what has occurred and the Readiness Team's assessment of the status.
- Based on this information, all teams will be asked if they are aware of other information or circumstances that need to be considered. The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing schedule or anything else, before proceeding to carry out their individual team functions. This is important in order that all teams understand all of the key issues. This will result in better coordination.
- Before any teams leave, the Emergency Coordinator will quickly review with each team leader the actions that each team will be taking. Team leader briefings will be done in the following order for the reasons indicated:
- Administrative Assistance - Because the Contingency Site is remote and requires travel, Company management must immediately begin making arrangements for the teams that will be going to the Contingency Site.
- Emergency Action Operations Teams - Needs to proceed to work with the Emergency Action Applications Team concerning work in progress and to coordinate with key users. As soon as those steps are complete, some or all of the team will travel to the Contingency Site.
- Emergency Action Applications Team - Needs to proceed to work with the Emergency Action Operations Team concerning work in progress and to coordinate with key users.

As soon as those steps are complete, some or all of the team will travel to the Contingency Site.

- Emergency Action Facilities Team - Needs to proceed to repair or replace the server room as required.
- Emergency Action Hardware Team - Needs to proceed to repair or replace the hardware as required.

K. Activating contingency site by emergency action operations team

These are the procedures for establishing operations at the Contingency Site.

Activating Contingency Site Procedures

- Before proceeding to the Contingency Site, the Emergency Action Operations Team must first coordinate with user departments to determine the status of production files and work in progress. In a case where the combination of work schedule, backup schedule, and offsite storage schedule results in serious loss of data or work already completed, large numbers of users, programmers, and Emergency Action Operations Team members will need to meet to evaluate alternatives. This needs to be accomplished before any of these people leave for the remote Contingency Site. Not all details may be resolved at this meeting because of time considerations. It may be appropriate for the Emergency Action Operations Team to go ahead and leave for the Contingency Site while the Emergency Action Applications Team remains to work with the users.
- Once the issues of lost data or lost work have been resolved to the point that the Emergency Action Operations Team can leave, the Team will prepare to leave for the Contingency Site as soon as possible.
- Upon arrival at the Contingency Site, the Emergency Action Operations Team will first organize all materials (tapes, documentation, hardware and supplies) in an area designated by Contingency Site personnel. For simplicity and control, the materials should not be spread out into many different areas but restricted to a single area if possible.
- Next, the Emergency Action Operations Team should refamiliarize themselves with the facility, the computer operations, and all security procedures to be observed.
- The Team Leader should remind the team members that all activities should setup a special log in addition to the Information Systems Log Form. Make sure everyone understands the importance of complete and accurate logging.
- When Contingency Site personnel have completed their setup preparations, the Emergency Action Operations Team will begin loading data on the hot-site machine. When loading the tapes, the tape drive must be set to 6250 bpi.
- Development files saved on the full backups do not need to be restored, only production software, data, and the operating system.

- If incremental backups since the above last full backup are intact, proceed to restore to appropriate directories. The incremental backups must be restored in chronological sequence.
- After the data, software, and operating system have been restored, the system will may need to be restarted.
- Conduct some simple tests of the applications to verify that the system is operational and working as expected.
- Coordinate with the Emergency Action Applications Team about their specific sequence of steps to recover lost work (data lost due to lost incremental backups and work in progress that was not completed or not backed up). If incremental backups could not be restored, data entered and processed since the last full backup may have been lost and may not be recoverable. However, source documents may be available so that the data can be reentered and reprocessed. If any case, it is the responsibility of the Emergency Action Applications Team to work with the key users to resolve what will be done.
- Once the recovery procedures have been worked out, the recovery work should be carefully scheduled with the Emergency Action Applications Team to ensure that recovery steps happen in a well-controlled sequence. Users will probably need to be present to verify results at each step. The Emergency Action Operations Team and users will probably need to be scheduled in shifts according to the work to be accomplished.
- When the key users have determined that the recovery work has been completed, the resumption of processing can be scheduled. Shift scheduling will need to be continued as appropriate.

L. Recovering lost work by emergency action applications team

The following procedures have been prepared concerning recovery of lost data and work in progress.

Recovering Lost Work Procedures - The Emergency Action Applications Team must coordinate with the users to first identify what work has been lost, if any, through lost incremental backups, lost source documents or other records, and lost work that was in progress and not backed up. Determination of status of all work is the first step that must be accomplished. As much of this process as possible should be done before leaving for the Contingency Site. The Team Leader should notify key users and call a meeting at the Emergency Control Center.

In the case of lost work and lost documents, the Emergency Action Applications Team should work with the users to determine the established plan for recovering the lost documents or the information contained in them. The recovery procedure may allow the lost data to be recovered in some fashion.

If data or work has been lost, the combined teams (Operations, Applications, and Users) must determine how the data or work will be recovered. This requires reviewing each application

carefully. In cases where data has been lost that is irrecoverable, some decision must be made as to what will be done to account for the lost information. This may mean lost dollars, lost business, or the inability to verify events with auditable records.

Once an action plan has been identified, it may be appropriate for Emergency Action Applications Team members and selected users to travel to the Contingency Site. However, if the recovery process is not difficult and communications are established rapidly, these personnel may be able to do their work remotely via communications links.

The lost work must be recovered as best possible with a combined effort of Operations, Applications, and the Users. This may involve around the clock efforts, doing data entry, correcting data files, running special jobs, or rerunning production jobs. In such a situation, all three groups will need to work in shifts to be scheduled by the Emergency Action Applications Team.

In the recovery process, if there are not enough people to work on all application areas simultaneously, then Company management must be careful to assign the work according to priorities of what is really important, the schedules that are most pressing, and the greatest impacts on the business, particularly survivability and profitability.

M. Coordinating users by emergency action applications team

It is the responsibility of the Emergency Action Applications Team to ensure that the applications systems work properly for the users, that lost work is recovered, and that the users understand the mode of interface during the recovery operation. The following are the user coordination procedures.

Procedures For Coordinating Users

- Upon completion of the joint disaster review meeting, the Emergency Action Applications Team's first priority is to determine the status of production files and work in progress. They will first coordinate with the Emergency Action Operations Team in this process.
- Depending on time of day, and point of time in the monthly schedule, the Emergency Action Applications Team will probably need to immediately get key users actively involved in the process of determining status. If so, key users will be notified and asked to meet at the Emergency Control Center.
- The Emergency Action Applications Team leader will brief the key users on the initial status situation, then divide employees up into groups by application system or subsystem, preferably with a mix of users, programmers, and operations staff in each group.
- When the issues of recovering most work have been ironed out, the Emergency Action Applications Team leader will coordinate a work schedule with the key users and the Emergency Action Operations Team leader. At this point, impact on ongoing work should

be carefully discussed so the key users clearly understand the situation and can give appropriate directions to their subordinates. User departments must understand what their interim work plans will be until their automated systems are recovered and back online.

- Once the recovery process is completed, the Emergency Action Applications Team will coordinate with the key users to ensure that they understand how they interface with their applications and what the restrictions are. If the numbers of terminals cannot handle the work load, users will need to work in shifts to take advantage of the available hours. However, the Emergency Action Operations Team leader must be involved in the scheduling to make sure processing conflicts are avoided. If unexpected problems are encountered, the Emergency Action Applications Team will work quickly to find solutions.

N. Hardware salvage or replacing by emergency action hardware team

The following procedures cover hardware salvage or replacement by the Emergency Action Hardware Team.

Hardware Procedures

- Our computer hardware was acquired from equipment vendors identified in Appendix C. In an emergency, our first resource for assessment of damage, repairability, and alternatives is with them. If repair is out of the question, loaner equipment may be immediately available. To speed delivery of new equipment, letters of intent may be on file with selected vendors (see Appendix D).
- In the event equipment can be repaired, Appendix D contains service agreements with F2OnSite's equipment vendors.
- Refer to the Appendix D for all applicable letters of intent. These letters have been approved by Company management and speed delivery of equipment to us during an emergency. Only the final configuration, purchase price, and/or current financing rates will need to be approved at the time of ordering the replacement equipment.

O. Facilities salvage or replacing by emergency action facilities team

These procedures cover salvage or replacement of the network server room facilities under the jurisdiction of the Emergency Action Facilities Team.

Procedures

- To work with Company management to identify options (repair existing or identify replacement) facilities.
- Work with outside vendors as appropriate for environmental, power and repair conditions.

P. Administrative coordinating by administrative team

The Administrative Team will determine the procedures for all administrative assistance regarding hotel arrangements, flight schedules, etc.

Administrative Coordinating Procedures

- Work with Company management to determine extent and duration of resources needed.
- Identify locations and individuals involved.
- Gather and provide the necessary resources.

Q. Specific procedures for user department contingencies

This section contains specific procedures for user interface and operation of their applications. The concept of the Contingency Site Coordinators necessary if a large number of information systems and user department staff must work at a Contingency Site.

Procedures For User Department Contingencies - The Contingency Site Coordinator will become familiar with the Contingency Site facility, determine if any aspects are inadequate for the situation at hand, and take necessary action. For example, if the staff accommodation capacity of the Contingency Site is exceeded, the Contingency Site Coordinator is responsible for arranging supplemental facilities. This could happen if an unusually large number of personnel are sent to the Contingency Site because of a disaster that prevents use of the planned communications arrangement. First choice in that particular case would be at the same hotel housing F2OnSite's personnel.

The Contingency Site Coordinator will represent the interests of the company as a whole rather than that of a specific department. He or she will review recovery plans and schedules to ensure that they are in line with the F2OnSite's operations priorities. If there are any doubts, especially if the F2OnSite's operations are affected significantly, the Contingency Site Coordinator will discuss the matter with the Emergency Coordinator who will take the issue to Company management.

During the recovery process and subsequent data processing and administrative operations, the Coordinator will facilitate the teamwork of the multiple departments. He or she will schedule shift work in the best interest of the company, will give pep talks or counseling to keep spirits up, and will be especially alert for team members becoming over stressed.

The Contingency Site Coordinator will stay in regular contact with the Emergency Coordinator to keep him or her current on status, progress, decisions made, unusual expenditures, and administrative matters.

R. Operating of application systems

These procedures address operation of the software applications from the Contingency Site.

Procedures For Operating Application Systems - If the planned communications facilities are established successfully, the operations of the business should be as normal except for some reduced numbers of PCs and related equipment. If this causes problems getting all work accomplished, the Emergency Action Applications Team and Emergency Action Operations Teams will assist with supporting staggered shifts so that a fewer number of PCs can handle the load. If other operational problems are encountered, the Emergency Action Applications Team is responsible to find solutions and to coordinate with the users about changes in procedures.

If the planned communications facilities cannot be established at the planned capacity for any reason (e.g. PCs are not operational, software does not run, etc.), the following actions will be taken:

- Heads of user departments will be responsible for sending selected users to the Contingency Site.
- Support of the systems will be accomplished by whatever means are possible, such as E-mail or voice communications to another location, couriers to the main office, etc.
- If branch offices are also unsupported with working PCs and printers, the Emergency Action Operations Team will assist the branch offices and interfacing departments to establish other methods of accomplishing the work, such as use of telephone, express mail, facsimile, etc.
- The key in unusual recovery situations is to be creative rather than panicked.

S. Procedures for replacing network server room

If the network server room is destroyed, steps will be taken immediately to establish a replacement network server room. A location must be found with adequate space; computer rooms must be constructed or modified; and computers, air conditioners, power distribution equipment, cabling, etc., must all be obtained and installed to prepare a working network server room.

Network Server Room Procedures

- The Emergency Action Facilities Team with assistance from the Emergency Action Hardware Team has procedures to identify potential replacement sites and probable means of obtaining equipment and facilities on an emergency basis.
- If equipment or facilities are salvageable, the Emergency Action Hardware Team and the Emergency Action Facilities Teams will assess what is usable or repairable and what needs to be replaced. The Emergency Action Hardware Team will initiate all salvage, relocations, and repair activities as necessary.

- The Emergency Action Hardware Team and the Emergency Action Facilities Team will initiate ordering of all new replacement equipment and facilities on an emergency (rush) basis. Financial, legal, and insurance issues must be considered during this process.
- As the new network server room is constructed and equipment arrives, the Emergency Action Hardware Team and the Emergency Action Facilities Team will coordinate obtaining permits, installation, wiring, etc., to ensure that the network server room is properly prepared.
- The Emergency Action Hardware Team and the Emergency Action Facilities Team will test the readiness of the new network server room. When it is ready, they will coordinate with the Emergency Action Operations Team to transfer operations from the Contingency Site to the new network server room.
- The network server room procedure will be complete when all problems with the new network server room have been resolved and operations have been restored at the new facility.

T. Procedures for returning to normal operations

The following procedures are for returning to normal operations after emergency (recovery) operations.

Returning To Normal Operations Procedures - The Emergency Coordinator must notify company management when information systems are transferred to the original network server room or to a new replacement network server room. As information systems are transferred back to normal operations, the recovery procedure will very quickly be phased down. The Emergency Action Operations Team must leave the Contingency Site with all property and materials belonging to the organization, and use due care and caution to protect all data and software.

The Emergency Coordinator and Readiness Team must maintain a full state of readiness during, and particularly after, returning to normal operations. The Emergency Action Operations Team will be directed to return materials back to their proper offsite storage, including current backup materials and media.

The Emergency Action Operations Team must inform all users that the emergency or disaster is over and that operations are now or soon to be returned to normal. The Emergency Control Center will be deactivated.

The final activity of the recovery process will be the meeting and debriefing of the Readiness Team, all Coordinators, and Emergency Action Team Leaders concerning the activities of the recovery. The Emergency Coordinator is responsible to make sure that events, problems and solutions, etc., are documented. Once documentation is complete, the Emergency Action Teams and Readiness Team can be deactivated. During the next review of the Plan, the

Emergency Coordinator will be responsible to ensure that any lessons learned are incorporated into the Plan.

XIII. Testing and Maintaining the Plan

After initial acceptance of this Plan, ongoing testing on a periodic basis is necessary to ensure the continued viability of its contents. This Plan must also be reviewed regularly and updated as necessary. This section deals with these issues by providing policies and procedures for testing this Plan and for periodic review and update.

A. Policies and procedures for testing

The organization will enforce the following policies and procedures governing testing of the Plan.

Plan Testing Policy - The Plan will be tested for procedural and organizational aspects as well as the technical ability to process information at the Contingency Site referenced in this Plan. Moreover, because it is important for the emergency teams to remain familiar with the recovery procedures, the Emergency Coordinator is responsible for conducting a test at the Contingency Site. The test will be performed each year and the results of the test will be reviewed and approved by Company management.

Plan Testing Procedures - Each year, in conjunction with reviewing and updating this Plan, the Emergency Coordinator must design, schedule and notify team members of the annual test. The test may vary from year to year, in order to evaluate different elements of the Plan, but at the least it must address all major procedures involving all Emergency Action Teams. The tests may be organized as several different tests during the year, each testing a different portion of the Plan.

The tests are to be regarded as review and training exercises as much as tests of the workability of the Plan. However, there will always be some features of the Plan that are truly tested. This means that the tests must be observed, measured, and all successes and failures recorded. The Alternate Emergency Coordinator will serve as the test monitor. During the progress of the test, if problems are encountered, solutions will be sought at that time.

At least in the initial acceptance tests (first year) and every two years thereafter, ALL critical applications will be tested to verify that no technical problems prevent those services from working. In intervening years, tests of critical applications may be staggered to reduce the complexity of the tests and the time required.

The tests will extend over a fairly limited time period so as not to have an undue impact on other business activities.

Following the tests, the Emergency Coordinator will document the results of the tests, including any recommended changes in the Plan. The test results will then be reviewed and approved by Company management.

Changes to this Plan, which result from the testing process, will be incorporated along with the changes from the annual review process.

B. Policies and procedures for review and update

The effectiveness of the Plan is impacted by changes in the environment that the Plan was created to protect. Some major factors that impact the Plan are: new equipment, changing software environment, staff and organizational changes, and new or changing applications.

The following policies and procedures have been developed to ensure that the Plan is reviewed and updated on a regular and reliable basis.

Plan Review And Update Policy - Once per year the Plan must be reviewed by the Emergency Coordinator and approved by F2OnSite management.

Plan Review And Update Procedures

- The Emergency Coordinator will appoint a review team of one or more people each year to review and update the Plan.
- When the review team has completed their review and update process, the Emergency Coordinator will also review and approve the revised Plan.
- Once approved by the Emergency Coordinator, the revised Plan will be submitted to Company management for final approval.
- The revised Plan (after review and update) will be used as the basis of the annual test. Updates must be distributed prior to the test. However, the tests themselves may also identify changes to the Plan; therefore, final distribution of updates will occur following the tests.
- The Emergency Coordinator will then direct the Alternate Emergency Coordinator to distribute the revisions to the Plan. For cost considerations, the revisions will be distributed as updates to the previous version.
- More frequent reviews/updates of the Plan may be initiated by the Emergency Coordinator, but shall require the approval of Company management because of probable impact on other projects.

XIV. Appendices

APPENDIX A - EMERGENCY NOTIFICATION LISTS

Emergency Service Numbers
Emergency Readiness Team
Company Management Succession Notification List

APPENDIX B - OFFSITE STORAGE AND CONTINGENCY SITES

Offsite Storage
Contingency Sites
Emergency Control Centers

APPENDIX C – VENDOR CONTACTS

Computer Equipment/Services
Communications Equipment/Services
Office Equipment/Services

APPENDIX D - SERVICE AGREEMENTS

APPENDIX E – INFORMATION SYSTEMS EQUIPMENT CONFIGURATIONS

Computer Equipment
Communications Equipment
Office Equipment

APPENDIX F – DISTRIBUTION LIST FOR THIS DOCUMENT

APPENDIX G – SUMMARY OF RESPONSIBILITIES

Appendix A – Emergency Notification Lists

<u>Description</u>	<u>Contact</u>	<u>Phone Number</u>
Emergency Services		
Police, Fire, Ambulance	Operator	911
Building maintenance		XXX-XXX-XXXX
Emergency Readiness Team		
Emergency Coordinator	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Alternate Emergency Coordinator	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Contingency Site Coordinator	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Emergency Action Teams		
Emergency Action Operations Team	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Emergency Action Applications Team	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Emergency Action Hardware Team	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Emergency Action Facilities Team	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Emergency Action Administrative Assistance Team	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Company Management Notification Succession List		
Executive	xxxxxx Address City, State Zip	XXX-XXX-XXXX
Finance	xxxxxx Address	XXX-XXX-XXXX

	City, State Zip	
Human Resources	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	

Appendix B – Off-site Storage, Sites, Emergency Control Centers

<u>Description</u>	<u>Contact</u>	<u>Phone Number</u>
Offsite Storage		
Provider	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	
	Acct #:	

The following items reside offsite:

- A copy of this Information Systems Business Continuity Recovery Plan
- Passwords (in a sealed envelope)
- Electronic backup media
- Diskettes
- Technical system documentation (system start up and shut down procedures)
- Blank checks

Contingency Site(s)

Location 1	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	
Location 2	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	
Emergency Control Center(s)		
Location 1	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	
Location 2	xxxxxx	xxx-xxx-xxxx
	Address	
	City, State Zip	

Appendix C – Vendor Contacts

<u>Description</u>	<u>Contact</u>	<u>Phone Number</u>
Computer Equipment/Services Server, PCs, printers	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Industry software	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Communications Equipment/Services Equipment (Routers, etc.)	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Communications lines (voice)	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Communications lines (data)	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Telephone systems	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Office Equipment/Services Fax machines	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx
Copiers	xxxxxx Address City, State Zip Acct #:	xxx-xxx-xxxx

Appendix D – Service Agreements

Included In This Appendix

- A copy of the Contingency Site service agreement. (Letter of Intent)
- A copy of the offsite storage facility agreement.
- Copies of all special recovery agreements with vendors, facilities providers, etc.

Appendix E – Information Systems Equipment Configurations

Computer Equipment Minimum Configuration

Network server minimum configuration:

• Preferred processor	XXXXXX
• Hard drive capacity	XXXXXX
• Memory (Ram)	XXXXXX
• Operating System	XXXXXX
• Keyboard, mouse	Yes
• Monitor size	XXXXXX
• Uninterruptible power supply (UPS)	Yes

Workstation system minimum configuration:

• Type (Desktop, Laptop, etc.)	XXXXXX
• Hard drive capacity	XXXXXX
• Memory (Ram)	XXXXXX
• Operating System	XXXXXX
• Keyboard, mouse	Yes
• Monitor/screen size	XXXXXX
• Security/anti-virus	XXXXXX
• Productivity suite	XXXXXX

Printer minimum configuration:

• Manufacturer	XXXXXX
• Minimum 12 pages per minute	XXXXXX
• Minimum resolution	XXXXXX

Peripheral equipment – not required unless specifically identified below
 Communications Equipment Minimum Configuration

Router Manufacturer	XXXXXX
Internet Connectivity	XXXXXX
Voice lines from telephone provider	XXXXXX

Telephone system

• Preferred Manufacturer	XXXXXX
• Preferred Model	XXXXXX

Office Equipment Minimum Configuration

• Preferred copier	XXXXXX
• Preferred fax	XXXXXX

Appendix F - Distribution List For This Plan

Position

Employee Name

Emergency Coordinator
 Alternate Emergency Coordinator
 Contingency Site Coordinator
 Emergency Action Operations Team Leader
 Emergency Action Applications Team Leader
 Emergency Action Facilities Team Leader
 Emergency Action Admin Assist Team Leader
 Offsite Storage

Appendix G – Summary of Responsibilities

Important locations

- Offsite storage
- Emergency Control Center
- Alternate Emergency Control Center
- Contingency Site

Readiness Team

- Emergency Coordinator
- Alternate Emergency Coordinator
- Contingency Site Coordinator
- Action Team Leaders

Emergency Action Operations Team
 Emergency Action Applications Team
 Emergency Action Hardware Team
 Emergency Action Facilities Team
 Emergency Action Administrative Assistance Team

Emergency Coordinator	Alternate Emergency Coordinator	Contingency Site Coordinator	Emergency Action Operations Team
Acts as liaison with fire, police, and remote offices	Implements emergency evacuation plans		
Coordinates efforts and directs all activities of Readiness Team	Activates and maintains Emergency Control Center	Activates and maintains Contingency Site	Obtains offsite storage materials and transports to Emergency Control Center and Contingency Site
Communicates recovery status to management	Communicates with Contingency Site	Communicates with Emergency Control Center	Initiates recovery efforts at Contingency Site
Reviews and oversees updates to Plan	Maintains up-to-date contact information for employees and vendors	Oversees new hardware/software, software updates	
Oversees Plan training	Monitors Plan testing and records progress	Participates in Plan testing	Participates in Plan testing
	Reviews backup procedures		

Emergency Action Applications Team	Emergency Action Hardware Team	Emergency Action Facilities Team	Emergency Action Administrative Assistance Team
Coordinates with users	Assesses damage to existing equipment	Assessing initial damages to facilities	Initially notifies employees
Assists in identifying data to be recreated	Recommends alternatives to repairing or replacng equipment	Recommends repairing existing offices or locating replacement facilities	Identifies housing and transporting requirements
Monitors recovery progress to determine systems are operating correctly	Orders and receives new/loaner equipment		Makes appropriate housing and transportation arrangements
Participates in Plan testing			Coordinates with employees

Appendix H – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Business Continuity Disaster Recovery Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

BUSINESS CONTINUITY OF OPERATIONS

DEPARTMENT PLAN

I. Purpose of the Business Continuity of Operations Department Plan

Business continuity ensures that critical processes will continue to perform service throughout an emergency or disruption. The purpose of this Business Continuity of Operations Department Plan (Plan) is to address the restoration of this department's business processes after a business disruption either internal, within the department, or external, outside of the department.

This Plan, along with the other Business Continuity documents, supports F2OnSite's Business Continuity Policy that provides overall guidance and direction for business continuity planning and related activities.

II. Overview of the Business Continuity of Operations Department Plan

F2OnSite has a large variety of processes whose continuous operations are critical to the organization's continuing viability. Business resumption planning involves arranging for emergency operations of these critical business functions and for resource recovery planning of these functions following a natural or man-made disruption.

This Business Continuity of Operations Department Plan is only one component of F2OnSite's business continuity planning process.

Each department provides important services to F2OnSite. Business continuity of operations plans are needed for all organizational units and include the logistics of workarounds should essential services (Internet, phones, software applications, etc.) not be available, getting personnel to work locations, temporary offices, recovery facilities, and housing.

This Plan contains:

- Workaround activities
- Backup resource arrangements
- Procedures for notification, activation, and emergency operations

III. Department Description

[Provide a brief description of this department]

IV. Preparing For A Disruption

A. IMPORTANT SERVICES AND PROCESSES

The first step in planning for a disruption is to identify important services provided within the department and externally outside of the department, and business processes that support such services. The purpose is to assist in formulating how this department will continue to perform critical functions and preserve critical assets during a disruption as well as to increase the level of departmental involvement in the formulation of the Plan.

This department performs the following important services and processes:

- Service/process
- Service/process
- Service/process

B. IMPORTANT RESOURCES

To perform the above services and process, this department relies on important resources and assets that exist within this department and externally outside of this department. Important resources should include IT related assets such as Internet, phones, specific software, etc.

Since a disruption can occur at any time, this department has identified manual recovery documents such as paper based data, forms, and procedures that should be stored off-site. These documents assist our department and minimize a business disruption. Information stored off-site includes:

- Description
- Description
- Description

This department relies on the resources and assets listed below. Include the person or department responsible for maintaining the resource or asset:

- Resource/asset & person
- Resource/asset & person
- Resource/asset & person
- Internet, IT Department
- Phone, IT Department
- Email, IT Department

- Software application A, IT Department
- Software application B, IT Department

C. DEPARTMENT DEPENDENCIES

This department relies on other departments within our organization. Describe the dependency and the department responsible for providing the service.

- Dependency and department
- Dependency and department
- Dependency and department

D. DEPARTMENT LEADERSHIP SUCCESSION

In the event of an emergency or disruption, personnel within our department should be contacted in the order listed below:

- Person and personal contact information
- Person and personal contact information
- Person and personal contact information
- Person and personal contact information

E. SPECIAL CONSIDERATIONS

Identify special considerations (geographic locations, inability to get in touch with staff, etc.) this department may face during an emergency or disruption:

- Special consideration 1
- Special consideration 2
- Special consideration 3

V. Disruption

A. NOTIFICATION

In the event of an emergency or disruption in service, the following notification procedures will be followed:

- Personnel will be contacted in the order listed in the Department leadership succession portion of this Plan. If no operations personnel are on duty, management has been provided with the proper procedures and notification process.
- Organization management and department management will make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.

B. INITIAL RESPONSE

Based on an assessment of the situation, the department manager will determine the severity of the problem to the department and decide on the appropriate action. Identify where:

- All personnel are to report during emergency operations
- Where to forward data and materials from off-site storage
- Other considerations

C. GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS

The appropriate correction, workarounds, or recovery steps will be implemented according to the severity of the emergency or disruption. This Plan includes procedures continuing business operations during a disruption. It also includes workaround procedures if the assets and resources are unavailable.

Important resource	Workaround procedures or alternate resource should important resource not be available
Asset/resource	
Asset/resource	
Asset/resource	
Asset/resource	
Internet	
Phones	
Email	
Software A	
Software B	
Software C	

D. DISRUPTION PROCEDURES

After the department personnel have been deployed, the department manager will track the location of our employees and continue to update the information throughout each day of the recovery operation.

Department personnel will create a log of daily events and tasks performed. This log will aid in recovery efforts as well as assist in a post disaster review of events.

Department managers will prepare written status reports on a frequent basis and, as requested by company management, keep them apprised of the current status.

E. RECOVERY STEPS

Once normal operations and important resource(s) have been restored, this department will take the steps listed below.

We will ensure that all materials have been collected from work areas. This includes both traditional paper documents as well as electronically stored information.

We will resume operations at the repaired facility or new facility as appropriate. Our departments shall follow the following operations procedures to ensure a smooth transition in this process.

- Recovery step 1
- Recovery step 2
- Recovery step 3

F. PLAN TESTING AND UPDATES

This Plan will be tested and updated on an annual basis. Following a disaster or disruption, we will document the events that transpired including any recommended changes to our procedures. The results will then be reviewed by company management.

Appendix A – Distribution List

President

Chief Operating Officer

Department Manger

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Business Continuity of Operations Department Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

BUSINESS CONTINUITY PLAN

I. Purpose of the Business Continuity Plan

Business continuity ensures that F2OnSite (F2OnSite) can continue to provide services during business disruptions. The emphasis for business continuity is on critical business processes that need to be recovered in the event of a disaster.

II. Overview of the Business Continuity Plan

Business continuity planning involves arranging for emergency operations of critical business functions and for resource recovery planning of these functions following a natural or man-made disruption.

This Business Continuity Plan is only one component of F2OnSite's business continuity planning process. Plans are needed for all organizational units and include the logistics of establishing policy, providing guidance, ensuring staff are trained on appropriate procedures, and ensuring testing and maintenance of the plan.

F2OnSite's business continuity process includes the following documents:

- Business Continuity Policy
- Business Continuity Plan (this document)
- Business Impact Analysis
- Business Continuity Disaster Recovery Plan
- Business Continuity Business Resumption Plan
- Business Continuity Communications Plan
- Business Continuity Operations Plans

III. Business Continuity Policy

F2OnSite's Business Continuity Policy provides overall guidance and direction for business continuity planning and related activities.

Business continuity plans are no longer a luxury, but an essential element of F2OnSite's risk management program. The decision to invest in business continuity is required by legislation, third parties (e.g., insurers), and the realistic view that management must minimize the impact of a disaster on business operations.

F2OnSite's Business Continuity Policy is in place to protect F2OnSite and its ability to continue business operations in the event of a disaster or component failure information assets. Business continuity requires management to identify risks and install the appropriate mitigating technologies.

An up-to-date Business Continuity Plan creates a competitive advantage out of its ability to respond to rapid changes in its environment. F2OnSite can then move from simple recovery to experiencing the benefits associated with the continuing of business operations that are in line with the corporate strategy of facilitating growth and profitability.

IV. Business Impact Analysis

F2OnSite's Business Impact Analysis (BIA) helps identify the business processes and applications that are essential to the survival of the business. The Business Impact Analysis identifies the amount of acceptable data loss (recovery point objective) as well as the speed at which systems must be restored (recovery time objective).

Business impacts are identified based on a worst-case scenario assuming that the infrastructure supporting each department has been destroyed and all records, equipment, etc. are not immediately accessible.

The Business Impact Analysis (BIA) identifies mission critical business functions and associated critical resources. Determining critical business functions and the impact on the organization is the first step in business continuity. The Business Impact Analysis:

- Identifies important business processes
- Determines processes critical to the business
- Estimates the potential impact and recovery timeframes
- Prioritizes critical processes

V. Business Continuity Disaster Recovery Plan

The primary objective of business continuity is to help ensure the operation of Company's business by providing the ability to successfully continue operations in the event of a disaster or emergency.

F2OnSite's management is responsible for protecting all assets of our organization. These assets include employees, physical property, information, and records relating to the conduct of the business.

Management personnel are specifically responsible for:

- Identifying and protecting all assets within assigned areas of control
- Ensuring that all employees understand their obligation to protect the organization's assets
- Implementing/observing security practices and procedures that are consistent with generally accepted practice and with the specific guidelines stated in this Plan
- Noting any variance from established security practices and initiating corrective action
- Assigning responsibilities for establishing, maintaining, and coordinating F2OnSite's Business Continuity Disaster Recovery Plan

The Business Continuity Disaster Recovery Plan documents the strategies, personnel, resources, and procedures required to provide immediate response and subsequent recovery from emergencies and disasters including:

- Unplanned business interruptions
- Loss of critical services (computer processing, telecommunications)
- Loss of building access (contamination, etc.)
- Physical facility catastrophe (fire, sabotage, etc.)

Specific goals of the Business Continuity Disaster Recovery Plan relative to a disaster or emergency include:

- To detail the correct course of action to follow
- To minimize confusion, errors, and expense to the Company
- To effect a quick and complete recovery of services

Secondary objectives of the Business Continuity Disaster Recovery Plan are:

- To reduce risks of loss of services
- To provide ongoing protection of company assets
- To ensure the continued viability of this Plan

VI. Business Continuity Business Resumption Plan

F2OnSite has a large variety of processes whose continuous operations are critical to the organization's continuing viability. Business resumption planning involves arranging for emergency operations of these critical business functions and for resource recovery planning of these functions following a natural or man-made disruption.

This Business Continuity Business Resumption Plan is only one component of F2OnSite's business continuity planning process. Business continuity operations plans are needed for all organizational units and include the logistics of getting personnel to work locations, temporary offices, recovery facilities, and housing. Employee safety orientation and insurance programs must also be included in business resumption planning.

F2OnSite's business resumption plan contains:

- Backup resource arrangements
- Procedures for notification, activation, mobilization, and emergency operations
- Resources at all facilities (permanent and temporary)

F2OnSite Company management will direct staff to implement emergency procedures. In most disaster situations, data will be lost. Departments must re-create lost data in addition to continuing existing business operations.

The Emergency Action Applications Team will coordinate with users and assist in identifying data that needs to be re-created. The Emergency Action Applications Team will also monitor recovery progress to ensure systems are operating correctly.

VII. Business Continuity Communications Plan

The Business Continuity Communications Plan provides procedures to coordinate communications within the organization, and between the organization, the media, and the public in the event of an emergency or controversial issue. Emergencies may include fires, bomb threats, natural disasters, or major crimes. Controversial issues may include police investigations, protests, or other situations that demand a public response.

The Business Continuity Communications Plan is not intended to change the way emergencies are initially reported. All emergencies should be reported immediately to management.

The Business Continuity Communications Plan not only addresses media relations and communications issues, but also includes procedures for the rapid identification of potentially harmful situations and the methods for responding to these situations quickly and effectively.

It is the goal of the Business Continuity Communications Plan to establish guidelines for dealing with a variety of situations, and to ensure that management and its authorized representatives are familiar with those procedures and their roles in the event of a disruption. The Business Continuity Communications Plan is designed to be used in conjunction with the normal decision making hierarchy of F2OnSite and does not supplant that decision making process. It is designed to be used in conjunction with operational crisis response plans managed through facilities, operations, and other units.

F2OnSite has a large variety of processes whose continuous operations are critical to the organization's continuing viability. The team leader of the Communications Team is responsible for:

- Factually assessing the situation and determining whether a communications response is warranted.
- Assembling the Communication Team that will make recommendations on appropriate responses.
- Implement immediate action to identify staff that should be informed about the situation, communicate facts about the situation, minimize rumors, and help restore order and/or confidence

VIII. Business Continuity Operations Plan

F2OnSite has a large variety of processes whose continuous operations are critical to the organization's continuing viability. Business resumption planning involves arranging for emergency operations of these critical business functions and for resource recovery planning of these functions following a natural or man-made disruption.

Each department shall have Business Continuity Operations Plans that orient employees who will be involved in activating the plan and performing emergency operations. Orientation material is also needed for all employees in both the life safety and Plan areas. Detailed emergency operations plans are needed:

- Before a disaster for use during testing
- After a disaster for use during emergency operations

While the IT Department is responsible for off-site storage of electronic data, all F2OnSite departments should evaluate manual recovery documents such as paper based data, forms, and procedures that must be stored off-site. F2OnSite departments will make the appropriate arrangements to ensure manual recovery documents, special forms, checks, etc. are stored off-site. These documents assist the individuals departments and minimize a business disruption::

- Contact lists. Departments should maintain emergency contact notification lists of all staff in their respective areas.
- Supporting information. In addition to the above, each department should maintain information, as appropriate, to assist in recovery operations. Backup resources such as locations and functions should be identified.
- Testing. Testing and training procedures should be developed.

Appendix A – Distribution List

President

Chief Executive Officer

All Department Heads

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Business Continuity Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

BUSINESS CONTINUITY POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Business continuity ensures that F2OnSite can continue to provide services during business disruptions. The emphasis for business continuity is on critical business processes that need to be recovered in the event of a disaster.

Business continuity plans are no longer a luxury, but an essential element of F2OnSite's risk management program. The decision to invest in business continuity is required by legislation, third parties (e.g., insurers), and the realistic view that management must minimize the impact of a disaster on business operations.

II. Purpose

The purpose of this policy is to protect F2OnSite's Information Resources and its ability to continue business operations in the event of a disaster or component failure. Business continuity requires management to identify risks and install the appropriate mitigating technologies.

An up-to-date business continuity plan creates a competitive advantage out of its ability to respond to rapid changes in its environment. With an effective plan, F2OnSite can move from simple recovery to experiencing the benefits associated with the continuing of business operations that are in line with the corporate strategy of facilitating growth and profitability.

III. Scope

This policy applies to all Staff that are responsible for continuing F2OnSite's business operations.

IV. Policy

The Chief Security Officer shall ensure:

- The organization has established, and implemented as needed, procedures to restore any loss of sensitive data stored electronically.
- A disaster recovery plan address issues specific to the operating environment.
- A disaster recovery plan addresses the data that is to be restored.
- A copy of the disaster recovery plan is readily accessible at more than one location.
- The organization has established, and implemented as needed, procedures to enable continuation of critical business processes and for protection of sensitive information while operating in the emergency mode.
- The disaster recovery plan balances the need to access the data with the need to protect the data.
- The disaster recovery plan identifies alternate security measures to protect sensitive information.
- The disaster recovery plan includes contact information for all persons that need to be notified in the event of a disaster, as well as roles and responsibilities of staff involved in the restoration process.
- Procedures for periodic testing and revision of contingency plans.
- Those responsible for performing contingency planning tasks understand their responsibilities.
- Staff performs tests of their procedures. The results of each test is documented and retained for audit purposes. The recovery plans are updated as a result of the tests.
- The organization assesses the relative criticality of specific applications and data in support of other contingency plan components.
- A Business Impact Analysis (BIA) formally documents risks and impact to the organization. The disaster recovery plan adequately mitigates business disruption risks.
- The organization has established, and implemented as needed, procedures that allow facility access in support of restoration of lost data under disaster recovery and emergency mode operations. Procedures allow facility access while restoring lost data. Procedures identify personnel that are allowed to re-enter a facility to perform data restoration. Procedures are also addressed in the organization's disaster recovery plan.
- Procedures for obtaining necessary sensitive information during an emergency. Procedures specify the staff members authorized to access sensitive information during an emergency.

F2OnSite shall develop and maintain a comprehensive Business Continuity Plan (Plan). This Plan encompasses both IT contingency planning as well as Company's corporate

office business unit contingency planning. This is not an IT-only undertaking and must cross all business functions and departments.

Company's risk assessment and Business Impact Analysis (BIA) provide the foundation for business continuity planning. The Business Continuity Plan should cover all essential and critical business activities. The Business Continuity Plan shall consist of:

- Business Resumption Plan – plan to resume business operations including logistics and steps to minimize risks.
- Disaster Recovery Plan - the technical aspect of business continuity planning; the advance planning and preparing necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.
- Communications Plan – the plan to communicate with employees, vendors, consultants, customers, service providers, and the media with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.

Business continuity teams shall include a minimum of the following:

- Readiness Team – maintains this Plan and manages business continuity activities
- Emergency Action Operations Team - initiates recovery efforts
- Emergency Action Applications Team - identifies data to be recreated
- Emergency Action Hardware Team - assesses damage, recommends alternatives
- Emergency Action Facilities Team – assesses facilities, repair or new offices
- Emergency Action Administrative Assistance Team

The Business Continuity Plan shall be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed. The Business Continuity Plan shall be tested at least annually and more frequently when changes in business processes or equipment necessitate a test.

The Business Continuity Plan shall be kept up-to-date to take into account changing circumstances. All staff must be made aware of the Business Continuity Plan and their roles.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Staff responsible for ensuring and restoring business operations.

Policy History

Version	Date	Description	Approved By
2.1	7/1/2020	Updated Initial policy release	

References:

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D),
164.308(a)(7)(ii)(E)
ISO 27001 A.12.3, A.17
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 AU-5, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-9, CP-10
NIST Cybersecurity Framework PR.IP-9, PR.IP-10, DE.DP-2, RS.RP-1, RC.RP-1,
RC.CO-1
PCI 12.10

BUSINESS IMPACT ANALYSIS

I. Introduction

A. PURPOSE

This Business Impact Analysis (BIA) helps F2OnSite (Company) identify the business processes and applications that are essential to the survival of the business. The Business Impact Analysis identifies the amount of acceptable data loss (recovery point objective) as well as the speed at which systems must be restored (recovery time objective).

Business impacts are identified based on a worst-case scenario assuming that the infrastructure supporting each department has been destroyed and all records, equipment, etc. are not immediately accessible. This Business Impact Analysis does not address recovery as these issues are addressed in the Business Continuity Plan and supporting documents.

This Business Impact Analysis (BIA) identifies mission critical business functions and associated critical resources. Determining critical business functions and the impact on the organization is the first step in business continuity. This Business Impact Analysis:

- Identifies important business processes
- Determines processes critical to the business
- Estimates the potential impact and recovery timeframes
- Prioritizes critical processes

During this process, the following were addressed:

- The systems and services important to the business
- The length of time Company can tolerate a business disruption
- The amount of information loss that can be tolerated
- The cost to the business in terms of losses to key systems or services

B. SCOPE

Our scope included an assessment and analysis of Company's business processes. To gather this information we used a questionnaire and interview process that asked a series of questions for each business unit area. After information was gathered from each business area, it was assembled and analyzed, and a prioritized list of systems and services was created.

The questionnaire and interview identified key sources of information and other resources for the organization. The intent was to identify:

- The financial impact resulting from the loss of a business function
- The non-financial impact due to an outage
- Critical points and resources required by various business functions

- Computer software applications
- Impact resulting from lost transactions/data
- Interfaces with external business partners

C. SUPPORTING INFORMATION

Interviews with the following departments provided supporting information for this Business Impact Analysis:

- Accounting and Finance
- Customer Service
- Human Resources
- Legal
- Marketing
- Production and Operations
- Sales

II. Business Processes

A. OVERVIEW

By interviewing key staff members, the Business Impact Analysis identified important business processes and associated critical resources. The process:

- Identified how quickly essential business units and/or processes needed to return to full operation following a disaster situation
- Identified the resources required to resume business operations

Business impacts were identified based on worst-case scenario that assumed that the physical infrastructure supporting each respective business unit had been destroyed and all records, equipment, etc. were not accessible for a range of time periods.

B. IMPORTANCE

Through interviews with the organization's staff, important business processes were identified. The importance of the business processes were classified according to its impact on the organization should the business process not be allowed to perform its service due to a business disruption. The following table summarizes the results of the interviews:

Department	Representative(s)	Process	Time when issue becomes High priority
Accounting/Finance	xxxxxx	Accounts Payable Lack of info for decisions	1 week 2 weeks
Customer Service	xxxxxx	Inbound call center phones	4 hours
Human Resources	xxxxxx	Payroll on processing day Benefits	2 hours 3 days
Legal	xxxxxx	Software Phones	2 days 2 days
Marketing	xxxxxx	Software Phones	2 days 2 days
Production/Operations	xxxxxx	Software Phones	2 days 2 days
Sales	xxxxxx	Receipt of RFP via email Sales inquiries	1 day 1 week

The above table provides a high-level overview of business processes provided by various departments. The time listed when the issue becomes a High priority is based upon either the department's inability to provide service or a high cost associated with the loss of the business process.

III. Financial Impact

A. OVERVIEW

The financial impact evaluated the loss to the department in the event of a disaster that resulted in the loss of a business process. Financial impact included various costs including:

- **Lost Revenue:** The loss of this business process resulted in lost revenue. This included the loss of customer revenue, missed collections, interest, etc.
- **Penalties:** The loss of this business process resulted in fines, penalties, or legal fees due to regulatory requirements (Federal, State, Local, etc.), change in credit rating, etc.
- **One time expense:** The loss of this business process resulted in one-time expenses including equipment, service provider, materials, etc.
- **Service:** A cost associated with maintaining service to the department's internal and external customers including temporary staff, overtime, etc.

- Recovery of lost transactions: Costs associated with re-creating transactions not available on backup media. In general, the event occurred some time after the last backup was stored off site. Costs included overtime, contracted third party, etc.
- Backlog: Overtime or additional staff required for the business process to address the backlog once the business process is restored.

B. FINANCIAL IMPLICATIONS

The table below provides a high-level summary of the financial costs to the organization should a business process not be able to provide services to its internal and external customers.

Department	Representative(s)	Comments	Anticipated financial impact or loss
Accounting/Finance	xxxxxx	xxxxxx	\$xxx,xxx
Customer Service	xxxxxx	xxxxxx	\$xxx,xxx
Human Resources	xxxxxx	xxxxxx	\$xxx,xxx
Legal	xxxxxx	xxxxxx	\$xxx,xxx
Marketing	xxxxxx	xxxxxx	\$xxx,xxx
Production/Operations	xxxxxx	xxxxxx	\$xxx,xxx
Sales	xxxxxx	xxxxxx	\$xxx,xxx

IV. Non-Financial Impacts

A. OVERVIEW

Company's business processes may have non-financial implications should a department be unable to provide services to its internal and external customers. Non-financial implications include:

- Legal ramifications or contractual agreements
- Quality of service to clients
- Loss of market share
- Fines, penalties, litigation
- Regulatory compliance

- Negative impact on personnel
- Other

B. NON-FINANCIAL IMPLICATIONS

The table below provides a high-level summary of the non-financial implications to Company should a department not be able to provide services. Business implications were obtained during interviews with the department representatives.

Department	Representative(s)	Comments
Accounting/Finance	xxxxxx	xxxxxx
Customer Service	xxxxxx	xxxxxx
Human Resources	xxxxxx	xxxxxx
Legal	xxxxxx	xxxxxx
Marketing	xxxxxx	xxxxxx
Production/Operations	xxxxxx	xxxxxx
Sales	xxxxxx	xxxxxx

V. Manual Procedures

A. OVERVIEW

The Business Impact Analysis interviewed business representatives to determine if departments had documented manual procedures that could be used as ‘workarounds’ in the event IT services were interrupted. Manual procedures can often be used by departments during short-term outages. Extended outages rely on our organization’s Business Continuity Plan to resume business operations.

B. BUSINESS CONTINUITY

The table below provides a high-level summary of departments with manual procedures that can be used during short-term business disruptions. Longer term disruptions may require activating the Business Continuity Plan.

Issues addressed included:

- Does your business function have documented manual procedures that could be used as ‘workarounds’ in the event IT services are interrupted? If so, are they stored off-site? When were the manual procedures tested or last used?
- If no manual procedures exist for your business function, estimate the number of workdays it would take to develop them.

Department	Formal procedures exist?	Stored off-site?	Last tested	Days to create procedures
Accounting/Finance	No	N/A	N/A	3 days
Customer Service	No	N/A	N/A	3 days
Human Resources	No	N/A	N/A	3 days
Legal	No	N/A	N/A	3 days
Marketing	No	N/A	N/A	3 days
Production/Operations	No	N/A	N/A	3 days
Sales	No	N/A	N/A	3 days

Most departments have informal workaround procedures if IT related services (data, phones, Internet, etc.) are not available. Departments providing important services should complete a Business Continuity of Operations Department Plan.

VI. Work Area Requirements

A. OVERVIEW

This Business Impact Analysis included the support requirements (space, furniture, office equipment, etc.) for departments in the event of an interruption in normal business operations (loss of facility, loss of IT processing etc.).

B. DEPARTMENT REQUIREMENTS

The table below provides a high-level summary of specific department requirements during a business disruption. Issues addressed included:

- The minimum number of employees required (critical personnel) to keep the business function operational to the point that the impact on the organization is minimal during a prolonged outage.
- In addition to employee requirements, there may also be unique work area business function resources (forms, contact lists, etc.) required at time of a disaster

Department	Minimal staff required	Other resources required
Accounting/Finance	2	Checks stored off-site
Customer Service	2	
Human Resources	10	Fax, copier
Legal	N/A	Need continuity plan
Marketing	2	Remote access
Production/Operations	50	Space for staff
Sales	2	Enroll forms stored off-site

Each employee is assumed to require:

- Desk
- Computer
- Phone
- Printer
- Internet access
- Email access

VII. Application Software

A. OVERVIEW

The Business Impact Analysis identified software applications required by departments to complete their business processes. Each employee was assumed to require Internet and e-mail access.

B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES

The table below provides a high-level summary of specific department requirements during a business disruption. Issues addressed included:

- *Importance* - High: high cost associated, must be recovered within a short period of time. Medium: medium to little cost associated, must be recovered. Recovery does not need to be immediate. Low: no stated cost, low visibility and can wait for recovery.
- *Recovery time objective* - the number of days or hours the business function can continue to function in an emergency mode without access to this application. It includes the overall time frame within which the business function or application system must be restored following the declaration of a disaster.
- *Recovery point objective* – the number of hours or days that users spent recreating or reentering lost data. The data can be re-entered based on source documents, or information from other sources. The recovery point objective dictates a backup strategy.

Software Application	Importance (high, med, low)	Recovery time objective (average)	Recovery point objective (average)
Accounting application	High	1 day	2 days of lost data
Software application 1	High	1 week	1 week of lost data
Software application 2	High	1 day	N/A
MS Office (Word, Excel, Outlook)	High	3 days	3 days of lost data
Company web site	High	1 day	N/A
Scanner software	Low	1 week	1 week of lost data

VIII. Third Party Services

A. OVERVIEW

The Business Impact Analysis identified third party service providers required by departments to complete their business processes. Each employee was assumed to require telephone and Internet access.

B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES

The table below provides a high-level summary of third party service providers used by Company's user departments. Issues addressed included:

- *Importance* - High: high cost associated, must be recovered within a short period of time. Medium: medium to little cost associated, must be recovered. Recovery does not need to be immediate. Low: no stated cost, low visibility and can wait for recovery.
- *Recovery time objective* - the number of days or hours the business function can continue to function in an emergency mode without access to this service provider. It includes the overall time frame within which the third party service provider must restore services following their declaration of a disaster.
- *Recovery point objective* – the number of hours or days that the data can be recreated following the loss of the service provider. The data can be re-entered based on source documents, or information from other sources. The recovery point objective dictates a backup strategy. The recovery point objective can vary from a business day to a month.

Service provider	Importance (high, med, low)	Recovery time objective	Recovery point objective
Answering service	High	1 day	N/A
Internet access	High	3 days	3 days
Service provider 1	High	3 days	N/A
Service provider 2	High	1 week	1 week
Service provider 3	Low	1 week	N/A
Service provider 4	High	2 days	2 days
Service provider 5	Medium	1 week	N/A
Service provider 6	Low	1 week	N/A

VIII. Information Technology

A. OVERVIEW

The Information Technology department provides application systems and technology required to support the organization's business processes. This includes application servers, e-mail servers, print servers, phone systems, and network services.

B. RECOVERY TIME AND RECOVERY POINT OBJECTIVES

The following table provides a detailed list of the software applications and services available to Company's users. The IT priority column represents IT's understanding of the importance of the application or service.

Software applications

Application Software	Server Name	Databases used	Full backup	Stored Off-site	Recovery time	IT Priority
Active Directory	XXXXXX		Yes	Yes	4 hr	High
Print Server	XXXXXX		Yes	Yes	4 hr	Medium
Internal Domain Name Server	XXXXXX		Yes	Yes	4 hr	High
External Domain Name Server	XXXXXX		Yes	No	4 hr	High
Exchange Mail Server	XXXXXX	Exchange	Yes	Yes	4 hr	High

External Mail Server	XXXXXX		Yes	No	4 hr	High
Fax Server	XXXXXX		Yes	Yes	8 hr	Medium
Accounting	XXXXXX	Many	Yes	Yes	8 hr	Medium
File Server	XXXXXX		Yes	Yes	12 – 24 hr	Medium
Voicemail Server	XXXXXX		Yes	No	12 – 24 hr	Medium
VPN Server	XXXXXX		No	No	4 hr	Medium
Backup Server	XXXXXX		Yes	Yes	6 hr	Medium
Web Server	XXXXXX		Yes	No	6 hr	Medium
Terminal Server	XXXXXX		No	No	8 hr	Medium

Important Third Party Service Providers (Internet, backup service, maintenance, consultants)

Vendor	Service provided	IT Priority
Service Provider 1	Internet access	High
Service Provider 2	Voicemail System Support	Medium
Service Provider 3	Phone Service Provider	High

IX. Summary

A. OVERVIEW

Risk can never be totally eliminated, but can be mitigated by the application of this Business Impact Analysis and Business Continuity Plan. The decision as to what level risk is acceptable is based on management's review of the residual risk that exists after controls have been implemented to reduce risks to acceptable levels.

This Business Impact Analysis provides management with an analysis of the financial and non-financial impact of a business disruption on various departments. Since the cost of providing redundant and fault tolerance IT solutions can be significant, it is important that management knows the impact of a business disruption on user departments.

B. IT ALIGNMENT

IT seems to be aligned with the needs of the users. The table below compares IT's time to restore availability against the needs of the users.

Software Application	IT time to restore application	User requirements (average)
Software application 1	8 – 12 hours	1 day
Software application 2	8 hours	1 week
Software application 3	8 – 24 hours	1 week
Software application 4	2 days	3 days
Software application 5	6 hours	1 day
Software application 6	3 days	1 week

Company's agreements with the following external service providers should be reviewed to ensure service levels and uptime are stated and are aligned with user department requirements.

Service provider	Recovery time objective (average)
Service Provider 1	1 day
Service Provider 2	3 days
Service Provider 3	1 week

C. DEPARTMENT RESPONSIBILITIES

IT should implement the following tiered approach to business continuity:

Strategic Approach	Approach	Advantages
IT equipment failure	Real time backup of information to Company off-site facility.	Immediate ability to restore data
Service failure	Ensure agreements provide stated availability (uptime) and guaranteed response times	Priority service aligned with users' needs
Data center or building failure	Use of formal data center service such as SunGard	Formal facility providing servers, work areas, Internet access

While the organization is vulnerable to business disruptions, most departments can continue some level of functionality even with highly diminished IT support. Based on the interviews, the vast majority of employees are aware of the issues surrounding business continuity.

User departments should:

- *Resources* - ensure that any special forms (checks, etc.) are stored off-site and are available in an emergency.
- *Equipment* - ensure that special equipment such as scanners, scanner software, etc. are available.
- *Procedures* – develop workaround procedures to maintain business processes in the event of IT service disruptions including loss of access to software applications, inability to access the Internet, phones not working, etc.

CAPACITY AND UTILIZATION POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Capacity and utilization safeguards are part of F2OnSite's risk management process to mitigate and reduce risks that can impact business operations and Information Resource availability.

II. Purpose

Capacity planning and utilization helps F2OnSite obtain maximum value from its Information Resources. In addition, planning ensures Information Resources meet current and projected needs.

III. Scope

This Policy applies to the Chief Security Officer, IT Director, and IT Operations Manager.

IV. Policy

For the purposes of this Policy, capacity and resource utilization is the extent to which F2OnSite uses its Information Resources. It is the relationship between output actually produced and the potential output that could be produced if Information Systems were fully used.

F2OnSite's Chief Security Officer (MGMT) is responsible for ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. The MGMT shall:

- Resources – identify important resources that should be monitored and measured.
- Requirements – prepare a list of capacity constraints that are relevant to important resources.
- Monitoring – describe the required resource monitoring, alerts to be issued, and actions to be taken.

The MGMT shall consider the following when determining the types of monitoring to be used:

- Automated tools – automated tools may be used to monitor capacity and utilization.
- Safeguards – review and evaluate policies, procedures, training plans and related controls and safeguards.
- Testing – testing may be used to identify system capacities and constraints.
- Monitoring logs – logs shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data.

The MGMT shall rely on the IT Department to review and document utilization statistics on data center equipment. Inefficient use of server resources shall be brought to the attention of the IT Director. See the Green Computing Policy for more information.

- The IT Department shall measure current capacity and performance on important resources identified by the MGMT. Measurements may be achieved through analysis of reports as well as statistical information produced by servers, firewalls, and related equipment. In addition, performance may also be measured using monitoring equipment.
- Resource monitoring and problem identification may use audit trails to detect disk failures, over utilization of system resources, network outages, and similar events. See the Audit Trails Policy for more information.
- The IT Operations Department is responsible for developing and maintaining backup procedures. Such procedures include notifying the System Administrator of any issues that require attention (e.g. failed backups, capacity issues, time to backup files, etc.). Since backups run unattended without operators present, sufficient storage capacity needs to be allocated for backups/media. See the Backup Plan for more information.
- The IT Department shall establish monitoring systems that can detect new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, and capacity planning. See the Security Monitoring Policy for more information.

The MGMT shall provide necessary capacity and utilization reporting to F2OnSite Executive Management on an as needed basis.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the MGMT, IT Director, and IT Operations Manager.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(7)(ii)(E), 164.308(a)(8)
ISO 27001 A.12.1.3
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 AU-4, AU-5(1), CP-2(2), SC-5(2)
NIST Cybersecurity Framework PR.DS-4, DE.DP-2
PCI 1.1.2, 1.1.5, 1.1.6, 1.2.1, 2.2

CERTIFICATION AND ACCREDITATION POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Security controls and safeguards are part of F2OnSite's risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

The formal process of Certification and Accreditation (C&A) ensures that a clearly established set of security requirements is developed and implemented and any residual risk is minimized and formally documented.

III. Scope

This policy applies to all Department Heads with authorized access to any of F2OnSite's Information Resources.

IV. Policy

The Certification and Accreditation is a standardized process to ensure that an information system meets documented security requirements throughout its life cycle. Validating security controls provides the following benefits:

- Demonstrates compliance with relevant regulations
- Establishes and formally documents security requirements
- Provides independent verification of the correct implementation of the security requirements
- Provides a formal risk analysis that documents residual risk once all of the security requirements have been met
- Important documentation for the assessed system is contained in one set of documents

Certification is the technical evaluation of the security components and their compliance for the purpose of accreditation. A certifier, usually an independent third party, audits a system for compliance with an established set of security requirements. Accreditation is

the formal acceptance of the adequacy of the system's overall security by F2OnSite management.

Through the use of Certification and Accreditation, the Chief Security Officer (MGMT) ensures that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The MGMT shall use the following guidelines when using Certification and Accreditation to evaluate F2OnSite's security controls.

Guidance – Define the list of standards or guidance documents to be used. The International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and other relevant frameworks help define a set of Security Requirements for the system.

Resources – Identify internal and/or external resources to perform the assessment.

Scope – Define the scope of the system being certified as well as its boundaries.

Security Requirements – Prepare a list of the security requirements that are relevant to the system. The security requirements are created based on the chosen guidance documents.

Description – Describe the system including mission description, system identification, criticality, etc. Document the environment including facilities, physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

Test procedures – Every security requirement must have one or more test procedures. Test procedures can include visual verification, interviews, balancing, and other means to validate the security requirement.

Certification – Where possible, the MGMT shall use Certified Information Systems Auditors to certify the security controls of F2OnSite's Information Systems. The auditor's report shall include their project scope, findings, and recommendations.

Risk Analysis – Once the security findings have been sufficiently addressed and verified, a Risk Analysis shall be performed to describe the severity of the residual risk. Residual risk is the risk that remains after security controls have been implemented.

Accreditation – Prior to delivery of the accreditation package to the approving authority, Department Heads may, at the discretion of the MGMT, make modifications to the security controls to minimize the risk of a denial of accreditation. When ready, the MGMT shall assemble and deliver a complete package to the designed approving

authority. The approving authority will either grant accreditation, grant an interim authority to operate, or denied accreditation.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO05.03, APO05.05, APO11.09-10, BAI01.03, BAI01.09, BAI07.02, BAI07.06
 GDPR Article 32
 HIPAA 164.308(a)(8)
 ISO 27001 9.2, A.12.7
 NIST SP 800-37 3.5
 NIST SP 800-53 AU-1, AU-3, AU-6, AU-9, AU-11
 NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.DP-2
 PCI A3.1.2.b, A3.2.2, A3.2.2.1, A3.2.3, A3.3.2

CHANGE MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's Information Resources are continuously becoming more complex with a dependency between resources. From time to time each Information Resource requires an outage for planned upgrades, maintenance, or fine-tuning. In addition, unplanned outages may occur that require upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

II. Purpose

The purpose of this policy is to manage changes in a planned and predictable manner so that Staff can plan accordingly. Changes require planning, monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of F2OnSite's Information Resources.

III. Scope

This policy applies to all Staff that installs, operates, or maintains Information Resources.

IV. Policy

Every change to an Information Resource (e.g. operating system, computing hardware, networks, applications, data centers) is subject to this policy and must follow appropriate change management procedures.

All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with appropriate department head.

A Change Management Committee, appointed by department heads, shall meet on a regular basis to review change requests and to ensure that change reviews and communications are satisfactorily performed.

A formal written change request must be submitted for all changes, both scheduled and unscheduled. All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change. The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, security implications, the timing of the change will negatively impact a key business process such as year end accounting, or adequate resources cannot be readily available (e.g. weekends, holidays, or during special events).

Resource owners shall be notified for each scheduled or unscheduled change. A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or unsuccessful. A Change Management Log Form shall be maintained for all changes. This log must contain, but is not limited to:

- Date of submission and date of change
- Owner and custodian contact information
- Nature of the change
- Indication of success or failure

Change management procedures shall:

- Ensure that production data is not unnecessarily replicated or used in non-production environments.
- Device configuration is backed up prior to implementing the change.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07

GDPR Article 25

HIPAA 164.308(a)(4)(ii)(C), 164.308(a)(8), 164.316(a)

ISO 27001 A.12.1.2, A.14.2.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 CM-3, CM-5, CM-9, SA-10

NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2

PCI 6.4

CLEAR DESK POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite has a responsibility to maintain high standards of security for private/non-public electronic information. F2OnSite data that is stored on or accessed by computers and other electronic devices must be secured against intentional or unintentional loss of confidentiality, integrity, or availability regardless of location. In addition, paper documents must also be secured and protected against unauthorized access.

II. Purpose

This policy protects F2OnSite's assets and helps ensure our ability to continue business operations.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

The Chief Security Officer (MGMT) shall ensure processes are in place to:

- Identify Sensitive Information (hardcopy and electronic) that must be protected from unauthorized access or disclosure.
- Identify workstations that must be shut down at the end of the work day vs. powered on at night so they can receive security updates.
- Laptops containing Sensitive Information must be secured per the Mobile Device Policy.

Staff shall ensure that sensitive or private/non-public electronic information is secured and removed from unauthorized disclosure or access when they leave their work areas. Staff who work with Sensitive Information should have lockable space available for

storage when information is not in use. Staff must check with their immediate supervisor or Company management if an employee is not sure what information must be locked up or what lockable storage is available.

When leaving their work area, users shall ensure that their desk and work area is clear (clear desk) of papers and removable storage media. In addition, monitors shall be cleared (clear screen) to protect against unauthorized access to information or Information Systems. Screen savers shall be automatically activated after a period of inactivity. See the Workstation Security Policy for more information.

Papers and electronically stored Sensitive Information (e.g. flash drives, laptops) must be locked in a drawer when Staff leave their desks. Storage areas containing Sensitive Information must be kept locked when Staff are away from their work areas. Keys to secure storage areas must not be left in the lock or accessible by unauthorized personnel.

To prevent unauthorized disclosure or access, devices that transmit or print (e.g. Fax machines, printers) Sensitive Information shall have the documents immediately removed from the device by an authorized individual.

Documents waiting to be shredded shall not be accessible by unauthorized personnel.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.07, APO07.05, APO12.02, APO12.07, APO14.02, DSS06.07
GDPR Article 25, 32
HIPAA 64.308(a)(4)(ii)(B), 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(B)
ISO 27001 A.11.2.9
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 AC-11, MP-2, MP-4
NIST Cybersecurity Framework ID.AM-6, ID.GV-4, ID.RA-3, PR.AC-2, PR.AT-1,
DE.DP-2
PCI 9.5, 12.5.5

CLOUD SERVICE PROVIDER POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite uses Cloud service providers to increase employee efficiency, improve our competitive edge, and enhance our image and reputation. Over the past several years, Cloud services have expanded so that almost any resource or service can be rapidly provisioned at low cost and with a minimal amount of effort.

II. Purpose

Cloud services provide convenient and on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services). The purpose of this policy is to establish the rules for the use of Cloud service providers, their responsibilities, and protection of F2OnSite information.

III. Scope

This policy applies to all F2OnSite staff. It applies to Cloud service providers that transmit, collect, store, process, manage, and dispose of F2OnSite's information.

IV. Policy

Cloud technology has expanded and allows almost any IT related resource to be offered as a service. By knowing the types of Cloud environments available, F2OnSite Staff can make informed business decisions. The following are examples of solutions offered by Cloud service providers:

- Anything as a Service (XaaS)
- Communication as a Service (CaaS)
- Database as a Service (DaaS)
- Infrastructure as a Service (IaaS)
- Monitoring as a Service (MaaS)
- Network as a Service (NaaS)

- Platform as a Service (PaaS)
- Security as a Service (SecaaS)
- Software as a Service (SaaS)
- Storage as a Service (STaaS)
- Voice as a Service (VaaS)

Examples of Cloud service providers include, but are not limited to, infrastructure (e.g. Amazon Web Services, GoGrid, Rackspace Hosting), platform (e.g. Google Apps, Salesforce), Internet mail systems (e.g. Yahoo!, Hotmail, Gmail), social media (e.g. LinkedIn, Facebook), storage (e.g. Google, Microsoft, Box), on-line backups (e.g. Carbonite, zip cloud), and related services.

When adopting a Cloud service provider technology, F2OnSite Staff shall consider the risks involved. A Risk Assessment shall be performed that identifies risks to the organization. A risk analysis shall be performed to determine the likelihood and impact of various events. A risk treatment plan shall be prepared that identifies preventive, detective, and corrective controls that reduce risks to acceptable levels. See the Risk Assessment Policy for more information.

Prior to entering into an agreement, F2OnSite Staff shall follow due diligence in selecting the Cloud service provider. This may include background checks of Cloud service provider and related personnel, length of time in business, experience with similar engagements, etc.

Staff shall ensure that the use of a specific Cloud service provider does not violate F2OnSite policies, procedures, agreements, and related documents. F2OnSite will provide an IT point of contact for the Cloud service provider. The point of contact will work with the Cloud service provider to ensure the Cloud service provider is in compliance with the above policies, procedures, agreements, and related documents.

F2OnSite IT Management shall maintain a list of all authorized Cloud service providers and the services performed by each. IT Management shall maintain copies of all agreements with Cloud service providers.

Agreements with Cloud service providers must specify:

- Confidentiality that protects F2OnSite's information as well as our customer information.
- Controlled access to F2OnSite information.
- How F2OnSite's information is protected by the Cloud service provider.
- Acceptable methods for the return, destruction, or disposal of F2OnSite information in the Cloud service provider's possession at the end of the agreement.

- The Cloud service provider must only use F2OnSite information and Information Resources for the purpose of the business agreement.
- Any other F2OnSite information acquired by the Cloud service provider in the course of the contract cannot be used for the Cloud service provider's own purposes or divulged to others.

Cloud service provider staff with access to F2OnSite Sensitive Information must be cleared to handle that information. Cloud service provider access to Sensitive Information shall be activated only when needed. Access shall be deactivated after services have been provided.

Cloud service provider staff shall report any security incidents directly to the appropriate F2OnSite personnel.

Upon Cloud service provider termination, the Cloud service provider shall ensure that all F2OnSite Sensitive Information is collected and returned to F2OnSite or destroyed within 24 hours. If requested by the F2OnSite Chief Security Officer (MGMT), the Cloud service provider shall return or destroy all F2OnSite information and provide written certification of that return or destruction within 24 hours.

Cloud service providers are required to comply with all State and F2OnSite auditing requirements, including the auditing of the Cloud service provider's work.

Agreements with Cloud service providers shall include explicit coverage of all relevant security requirements. Agreements shall include controls over the processing, accessing, communicating, hosting or managing the organization's Information Resources or adding or terminating services or products to existing information. Agreements shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

Agreements with Cloud service providers shall specify that the service provider will notify F2OnSite within 72 hours of discovery of a Cloud service provider security breach. Upon such notification, F2OnSite shall have the right, but not the obligation, to terminate the agreement with the Cloud service provider. If the Cloud service provider had access to F2OnSite customer information, the Cloud service provider shall pay for all costs incurred to remedy the breach including, if appropriate, notifying F2OnSite's customers, paying for one year of free credit report for F2OnSite's customers, and related expenses.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO01.11, APO09.05, APO10.05, APO11.09, APO13.07, DSS01.05
GDPR Article 24, 28
HIPAA 164.308(b)(4), HITECH ARRA 13402
ISO 27001 8.3, A.5.1.1, A.17
NIST SP 800-37 Appendix G
NIST 800-53 CP-2
NIST Cybersecurity Framework ID.SC-4-5, DE.CM-6, RS.MI-2
PCI 2.6, 3.5.1, 3.6, 8.2.3 - 8.2.5, 8.5.1, 10.8

COMPLIANCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite values its relationships with our employees, customers, service providers, regulators, and the business community. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

II. Purpose

A strong compliance program provides our organization with a competitive advantage, helps protect our image and reputation and reduces costs. By establishing and maintaining a compliance management framework, we comply with company specific and statutory regulations.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Executive management is responsible for F2OnSite compliance with all relevant laws and regulations, compliance processes, and related reporting requirements. Executive management must create an environment of individual and collective accountability that includes the importance of meeting compliance obligations. Executive management must provide sufficient resources such as training, budgeting and staffing, to ensure compliance with company specific and statutory regulations.

Complying with applicable laws, regulations, and standards is the responsibility of every Staff member. The Compliance Department shall identify and communicate minimum compliance requirements for each Staff member and their business activities. Staff must know, understand, and meet compliance requirements that govern daily business activities.

The Compliance Department shall:

- Create, review, and update policies and procedures.
- Monitor departments to ensure compliance with requirements.
- Keep abreast of regulatory and industry trends to identify new compliance requirements and related changes to F2OnSite business processes.
- Track and communicate to executive management issues encountered, lessons learned, and changes required.
- Ensure the on-going evolution of compliance management to ensure relevance and strategic competitive advantage.
- Ensure accurate and timely reporting to executive management.

When executive management, legal, or other appropriate Staff perceives a compliance issue, the Compliance Department shall investigate and make recommendations regarding any actions or concerns.

F2OnSite's executive management, compliance, legal, and audit functions are actively involved in managing compliance related risks:

- Management - develops and implements mitigation activities, including monitoring and reporting, for managing compliance in business activities.
- Compliance – the Compliance and Legal Departments monitor related laws, regulations, and standards. The Legal Department translates the laws into compliance obligations and assists in identifying compliance requirements.
- Audit – the audit department provides management with independent, objective assurance on the overall effectiveness of the design and operation of internal controls and activities.

The Chief Security Officer shall ensure:

- The organization has established a plan for outside, independent, periodic technical and non-technical evaluation of IT systems.
- No less than annually, IT systems shall be reviewed by an outside, independent organization to ensure F2OnSite maintains reasonable and appropriate security measures. Such review shall include a review of internal and external systems, people, and processes.
- Evaluation reports, analysis, recommendations, and subsequent changes are fully documented.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all company management, the Compliance Department, the Legal Department, MGMT, and the Audit Department.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.03, APO01.11, MEA02.11, MEA03.01, MEA04.11

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(8)

ISO 27001 A.18

NIST SP 800-37 3.5

NIST SP 800-53 All XX-1 controls (e.g. AC-1)

NIST Cybersecurity Framework ID.GV-3, ID.SC-4, PR.PT-1, DE.DP-2

PCI 11.2, 12.4.1, 12.8.4

CONFIGURATION MANAGEMENT PLAN

I. Introduction

Configuration management is an on-process of identifying and managing changes to Information Resources. Configuration Items are Information Resources that are to be placed under configuration control. This Configuration Management Plan:

- Provides information on the requirements and procedures necessary for configuration management activities
- Establishes the methodology for configuration identification and changes to Configuration Items
- Describes the process for maintaining status and verifying the completeness and correctness of Configuration Items

II. Purpose of the Configuration Management Plan

This Configuration Management Plan (Plan) describes how configuration management is conducted throughout a lifecycle. This includes the responsibilities, procedures, activities, and oversight necessary to provide configuration identification, change control, status accounting and configuration audits.

This Plan documents and informs project stakeholders about configuration management, tools used, and how they will be applied by the project to promote success. The Plan defines methods for:

- Identifying baseline configurations
- Controlling modifications and releases
- Reporting and recording status of requested changes
- Ensuring completeness, consistency, and correctness
- Controlling storage, handling, and delivery

The intended audience of this Plan is ABC Executive Management, Chief Risk Officer, and Chief Security Officer.

III. Roles and Responsibilities

A. INTRODUCTION

ABC Company cannot protect the confidentiality, integrity, and availability of information without ensuring that all Staff involved in changes to Information Resources:

- Understand risks related to changes to Information Resources
- Understand Staff roles and responsibilities
- Understand ABC Company's security policies and procedures designed to manage and mitigate risks to Information Resources

B. CONFIGURATION MANAGEMENT COMMITTEE

A Configuration Management Committee (Committee) consists of ABC Company's Risk Management Officer, Chief Security Officer, and IT Director. The Committee:

- Receives change requests
- Seeks clarification on any change request (if needed)
- Reviews and approves/rejects configuration change requests
- Ensures that approved changes are added to a Configuration Management Database

C. CONFIGURATION ITEMS

The Committee identifies specific Configuration Items from the list below:

- Communications – cell phones, voice mail, e-mail, Fax, Internet, etc.
- Facilities – access controls, alarms, etc.
- information – collected, transmitted, and stored, databases, etc.
- Information systems (hardware) – workstations, servers, networking equipment (routers, switches, hubs, access points, etc.), load balancers, important peripherals, backups, etc.
- Information systems (software) – operating systems, software applications, utilities, etc.

D. BASELINE CONFIGURATIONS

The Committee ensures that each Configuration Item is added to the Configuration Management Database. The Configuration Management Database includes relevant information about the Configuration Item including a description, Resource Owner, attributes, baselines, relationships, changes, and other important information.

A baseline configuration is established for each Configuration Item. A baseline is a collection of information describing the technical characteristics of each Configuration Item. Baselines serve as technical control points in a resource life cycle for the evaluation of proposed changes to the Configuration Item. The baseline and the approved changes or modifications provide a current description of the system. Major baseline configuration elements can include:

- Configuration Item name
- Functional purpose
- Resources needed
- Interfaces between internal and external resources
- Documentation – technical, operational, design, users, maintenance, etc.

- Change history

IV. Configuration Control

A. PROCESS OVERVIEW

Configuration Control involves systematically controlling and managing configurations throughout an Information Resource lifecycle. Configuration Item change requests are initially sent to the Resource Owner for review and authorization. If authorized, the Resource Owner sends the change request to the Committee.

When reviewing change requests, the Committee considers the risk to the organization, cost, timing, and impact of the change. Only necessary changes are approved by the Committee. This configuration control process ensures that Configuration Items are handled in a consistent manner.

B. APPROVED CHANGE REQUESTS

Once approved by the Committee, approved change requests are entered into a Configuration Management Database with a “Requested” status. The change request is then sent to the appropriate department for implementation and resolution. The department that implemented the change will send status (i.e. “Completed” or “Fail”) notification to the requestor, Resource Owner, and the Committee. The Configuration Management Database is then updated with the current status of the change.

Once notified that the change is in place, the Resource Owner arranges for appropriate:

- Testing of the change to ensure the Information Resource operates as desired
- Changes to documentation (if needed)
- Training of Staff (if needed)

It is important that the Risk Management Officer, Chief Security Officer, Director of IT, and Resource Owners have the ability to review configuration status at any given time. The Configuration Management Database ensures that Staff are working off of the same information and have access to the latest updates. Access to the Configuration Management Database is controlled:

- The Committee determines who has read and write access to the Configuration Management Database
- The Resource Owner determines Staff that have read access to the Configuration Management Database

V. Configuration Management

A. OVERVIEW

The Configuration Management Database is a central repository of Configuration Items. As Configuration Items go through various stages of collection, processing, and reporting, the Configuration Management Database has the most current information available.

B. CONFIGURATION MANAGEMENT DATABASE

The Configuration Management Database may include information on approved configuration documents, software, version numbers, data, relationships, status of submitted change requests, and configuration audits. The Configuration Management Database provides information on:

- Change requests. When request was initially submitted, department submitting request, and Information Resources involved.
- Versions. Information Resource current and prior versions.
- Relationships. Resources required, Configuration Item relationships.
- Configuration Management Audits. The information in the Configuration Management Database is accurate and complete.

C. CONFIGURATION STATUS ACCOUNTING

Configuration management processes ensure the proper recording and reporting of Configuration Items. This includes the status of Configuration Items, proposed changes, the implementation status of approved changes.

Configuration status accounting identifies a Configuration Item's current status and lifecycle. A Configuration Status Report may include:

- Specifications that describe each Configuration Item
- A list of Configuration Items that comprise a baseline
- Configuration Item dates when each version was baselined
- History of baseline changes including rationales for change
- Configuration Item status with approved change requests
- A list of open change requests by Configuration Item
- Configuration audit list of deficiencies and non-conformities

VI. Configuration Management Audits

A. AUDIT PROCESS

Configuration management audits (Audits) help ensure the integrity of the Configuration Management Database is maintained. Audits ensure:

- Configuration management processes are being followed
- Recorded changes/updates were properly approved
- Configuration Items have been properly identified
- Information in the Configuration Management Database is accurate and complete

Audits are performed by independent Staff that not part of production operations. The audits are performed on an annual basis and after a major change or update to Information Resources. Deficiencies and non-conformities are identified in the Configuration Management Audit Report (Audit Report).

Processes

The Audit includes an evaluation of configuration management processes to ensure they are followed as specified in configuration management policies and plans. Such processes include:

- Change request – initiation, approval or rejection, modifications, and completion
- Configuration Item – additions, changes, and modifications

Approvals

The Audit verifies Resource Owners have approved each change request, the Committee has performed a risk assessment of the change request and approved each change, and the status of each change request is noted in the Database.

Also included in the Audit is a review of installed software against the Database to identify unlicensed or unauthorized software.

Accuracy

The Audit reviews information in the Database to verify it is complete and error free. The Audit reviews:

- Configuration Items to ensure the Database is complete and agrees with an inventory of Information Resources
- Baselines to verify they agree with actual Information Resource configurations
- Documentation is complete and includes maintenance requirements, licenses, warranties
- Configuration Item history, versions, timestamps, and change control integrity
- Configuration Item data is accurate and complete
- Adherence to requirements, standards, and service level agreements
- Changes were tested prior to moving changes/updates into production
- Safeguards during change

- Processes to back out or reverse a change or implementation
- Notification after change

C. AUDIT REPORT

Any deficiencies and non-conformities from configuration management policies, plans, and procedures are identified in the Audit Report. The Audit Report is distributed to the Committee so that appropriate action can be taken.

The Committee will identify the corrective actions necessary to resolve the deviations and assign responsibility for each corrective action to a person/department. As actions are taken, notes are added to the Configuration Management Database so a full history is available.

Appendix A – Distribution List

Risk Management Officer

Chief Security Officer

IT Director

All Resource Owners

Appendix B – Receipt and Acknowledgement

I have read ABC Company's (Company's) Configuration Management Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

CONFIGURATION MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's Information Resources provide our organization with the tools needed to accomplish our objectives and meet our obligations. Information Resource configurations must be planned and managed to optimize resources, mitigate risk, and maximize return on investment.

II. Purpose

The purpose of this policy is to establish a configuration management program that identifies responsibilities and requirements for a configuration management process designed to safeguard F2OnSite's Information Resources.

III. Scope

This policy applies to F2OnSite's Risk Management Officer, Chief Security Officer, and Director of IT.

IV. Policy

A. RISK MANAGEMENT

Executive Management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. F2OnSite's Risk Management Officer (RMO) shall ensure a formal and documented Risk Management Framework has been established to manage risks related to Information Resources. For more information see the Risk Management Policy.

B. CONFIGURATION MANAGEMENT PROCESSES

A Configuration Management Committee (Committee) shall consist of F2OnSite's Risk Management Officer, Chief Security Officer, and IT Director. The Committee shall develop, implement and maintain configuration management processes.

Configuration management processes shall ensure:

- **Baselines.** Information Resources configuration baselines shall identify specifications that have been formally reviewed and agreed upon. Baselines shall only be changed through change control procedures. Examples of baseline configurations include logical placement within the organization, network topography, model, version, connectivity and interactions, etc.
- **Changes.** Changes and updates (including patches) to Information Resources shall be implemented only with approval of the appropriate Resource Owner.
- **Recover.** Prior to authorizing a change to an Information Resource, processes to back out or reverse a change or implementation shall be identified. Previous baseline configurations shall be retained to assist in a rollback.

Configuration and change management processes shall incorporate applicable industry best practices, which support Information Resource availability, integrity, and confidentiality. Recommended practices include:

- Use of standardized and documented methods, processes, and procedures
- Making informed risk-based decisions
- Tracking and communicating to relevant parties changes to Information Resources

A Configuration Management Database shall be implemented and maintained with relevant information about the Information Resource including a description, Resource Owner, attributes, baselines, relationships, changes, and other important information.

C. CONFIGURATION MANAGEMENT CHANGE CONTROL

Changes to systems and application programs shall be managed to protect the systems and programs from failure as well as security breaches. System change control processes shall be implemented and maintained.

The Committee shall ensure the following preparation activities are performed:

- Develop and enforce formal change control procedures
- Analyze changes to Information Resources to determine potential security and privacy implications
- Ensure Information Resources are safeguarded during change and emergency change
- Review and approve proposed changes to Information Resources
- Test Information Resource updates prior to moving changes/updates into production
- Ensure only authorized personnel are permitted to implement changes

The Committee shall ensure the following documentation activities are performed:

- Document change including date, time, Information Resource involved, actions taken, success/failure, and other important items
- Retain records of changes to the Information Resource for the life of the Information Resource

As needed, role-based training shall be provided to appropriate Staff and shall include new features, security implications, changes in business processes, documentation, and other relevant factors.

The MGMT shall ensure physical and logical access restrictions are implemented to manage changes to Information Resources. See the Change Management Policy for more information.

D. SECURITY/PRIVACY IMPACT ANALYSIS

When there is a material change to an Information Resource, or a security/privacy implication has been identified, the Risk Management Officer (RMO) shall ensure a security/privacy impact analysis is conducted. Such impact analysis to include:

- Identification of applicable regulatory or compliance requirements (see the Compliance Policy for more information)
- Data classification (see the Data Classification Policy for more information)
- Risk management and risk mitigation considerations (see the Risk Management Policy for more information)
- Additional change management approvals required

E. CONFIGURATION SETTINGS

Configuration settings are parameters that can be changed in Information Resource hardware, software, or firmware. The MGMT shall ensure that controls manage changes to configuration settings:

- A standard set of mandatory configuration settings shall be established, maintained, and documented
- Configuration settings shall reflect the most restrictive mode possible while ensuring the Information Resource meets operational requirements

The MGMT shall ensure each Information Resource provides only the essential features/capabilities needed and specifically prohibits or restricts services not required. For more information on networks, see the Network Configuration Policy.

Information Resource configurations shall be compared against approved security configurations defined for each device. If any deviations are encountered, an alert shall be issued and appropriate action taken.

F. CONFIGURATION MANAGEMENT PLAN

The MGMT shall ensure a Configuration Management Plan (Plan) is developed and maintained. The Plan shall document and inform project stakeholders about configuration items, baseline configurations, change requests, configuration management database, configuration status accounting, and configuration management audits.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite's Risk Management Officer, Chief Security Officer, and Director of IT.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO12.02, APO13.07, BAI05-03, BAI05-08, BAI06-06, BAI07-06, MEA03-01
GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(8)

ISO 27001:2013 A.12.1.2, A.14.2.2-4

NIST SP 800-37 3.3, 3.4, 3.7

NIST SP 800-53 CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7

NIST Cybersecurity Framework ID.BE-4, ID.RA-4, PR.AC-4, PR.DS-3, PR.IP-1, PR.IP-3, DE.AE-1

PCI 6.4.6, 12.11, A3.2.2.1

CONTEXT AND ALIGNMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Executive Management is responsible for the design of F2OnSite's corporate strategies. Operational managers and Information Technology (IT) must be properly aligned with corporate strategies and the needs of the organization.

II. Purpose

IT alignment helps ensure that the organization properly manages its IT projects, service delivery, risks, and meets compliance requirements.

III. Scope

This policy applies to F2OnSite's Executive Management and department heads.

IV. Policy

F2OnSite strategies and culture is enabled as a strategic asset when there is an understanding and consistent implementation of organization values, policies, and procedures.

Each department shall:

- Create goals that contribute to achieving organization objectives.
- Document how the goals are aligned with the organization.
- Prepare action plans including people, processes, procedures and products that outline steps to implement department goals.
- Assign staff to track and monitor implementation of the action plan. Prepare quarterly status reports for Executive Management.

Executive Management shall:

- Review and approve department action plans.
- Review quarterly action plan status reports and provide feedback as necessary.

The Information Security Management System (ISMS), action plans and status reports shall include internal and external issues that are relevant to F2OnSite. The IT Director shall determine the effect of the issues on the organization's ability to achieve the intended outcomes of the ISMS.

The IT Director shall determine interested parties and Data Owners that are relevant to the ISMS. In addition, the IT Director shall determine the requirements of the interested parties and Data Owners relevant to the ISMS. The requirements of the interested parties and Data Owners should include contractual obligations as well as legal and regulatory requirements.

The IT Director shall determine and document the scope of the ISMS by reviewing the boundaries and applicability of the ISMS. When determining the scope, the IT Department shall consider:

- Internal and external issues that affect the intended outcomes of the ISMS.
- The requirements of the interested parties and Data Owners.
- Interfaces and dependencies between activities performed by the organization and those performed by other organizations.

The IT Director shall ensure that an ISMS is implemented, maintained, continually improved, and is aligned with the needs of the organization.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Executive Management and the IT Director.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM02.03, APO01.03, APO01.11, APO02.08, BAI01.03, DSS01.05
GDPR Article 24
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(8)
ISO 27001 4, 6, 10
NIST SP 800-37 3.1, 3.2, 3.5
NIST SP 800-53 AT-2, AT-3, CM-2, CM-3, CP-3, IR-2, PL-2, PM-13, SI-4
NIST Cybersecurity Framework ID.RA-1, ID.RA-6
PCI 12.8.4, A3.2.1

COVID-19 RESPONSE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

The Company's response to COVID-19 shall be of a general and a geographic response to the current conditions, and local laws and regulations.

II. Purpose

Covid-19 is a pandemic that can be mitigated by several factors, of those factors, the most pressing is social distancing and the use of Masks or other Personal Protection Equipment (PPE).

III. Scope

This policy applies to all staff, field, onsite and corporate employees.

IV. Policy

All Employees shall strictly adhere to all local, state and federal regulations regarding social distancing and the use of PPP, along with any other safety procedures as outlined by authorities. Furthermore, all Employees shall adhere to 'site policies', whereby additional requirements may be implemented or required. Examples would be buildings where Masks are required; in such cases Employees should adhere to the most stringent of the regulations, i.e. if Local regulations do not require a mask to be worn, but a particular entrance to a building does, the Employee must wear a mask (or adhere to the more stringent policy)

F2OnSite shall not be held responsible and shall hold no liability to any Employee or entity in contracting COVID-19. The risk of contracting the virus is held by the Employee or others, not by the Company.

Preferably, PPE shall be used in all instances during any customer contact, or at any time you are in public. PPP shall include, but are not limited to the following:

- Masks
- Latex Gloves (non-latex gloves are acceptable – medical grade)
- Faceshields where required
- Hand Sanitizer

Proper usage of masks can be located and reviewed here:

<https://www.cdc.gov/coronavirus/2019-ncov/downloads/hcp/fs-facemask-dos-donts.pdf>

One option for obtaining PPP can be located here: <https://www.amazon.com/Best-Sellers-Home-Improvement-Personal-Protective-Equipment-Safety-Gear/zgbs/hi/486555011>

There are key elements of social distancing and Covid-19 protection including but not limited to the following:

- Maintain six feet distance from others
- Maintain a sanitary work area, using antimicrobial wipes before and after utilizing any work area.
- Do not shake hands or ‘fist bump’ with others.
- Leave your mask in place and do not remove it during your stay onsite.
- If you use a cloth, wash your mask daily.
- Use hand sanitizer before and after your visit to the customer site.

“What happens if I become exposed?”

1. Quarantine yourself immediately
2. Contact your doctor
3. Locate your nearest testing facility
4. Notify your manager
5. Keep others away from you.
6. Adhere to local and state regulations and recommendations.
7. Review the following: https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/quarantine.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fcoronavirus%2F2019-ncov%2Fif-you-are-sick%2Fquarantine-isolation.html

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Employees.

Policy History

Version	Date	Description	Approved By
2.1	7/1/2020	Updated Initial policy release	D Lauderback

References:

<https://www.cdc.gov/coronavirus/2019-ncov/index.html>

<https://www.cdc.gov/coronavirus/2019-ncov/hcp/using-ppe.html>

<https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public>

CYBERSECURITY FRAMEWORK POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

A Cybersecurity Framework is a set of industry standards and best practices that help organizations cost effectively manage cybersecurity risks.

II. Purpose

Information Resources are critical to F2OnSite's business operations. This policy ensures a cybersecurity framework will be developed and implemented using business drivers to guide cybersecurity activities and protection mechanisms.

III. Scope

This policy applies to all F2OnSite Staff that have a responsibility to manage risks related to F2OnSite's Information Resources.

IV. Policy

A. CYBERSECURITY FRAMEWORK FUNCTIONS

A cybersecurity framework allows communication of cybersecurity activities and outcomes across a wide range of F2OnSite departments from Executive Management to operational departments. The following functions provide a strategic view of F2OnSite's lifecycle management of cybersecurity risk:

- Identify
- Protect
- Detect
- Respond
- Recover

Identify. F2OnSite Staff shall understand and manage cybersecurity risk to systems, assets, data, and capabilities. Understanding business risk, resources that support

critical functions, and the related cybersecurity risks enables F2OnSite to focus and prioritize our efforts in a manner that is consistent with our risk management strategy and needs of the organization. Major categories to achieve these objectives include:

- Asset Management – Information Resources that enable F2OnSite to achieve business purposes shall be identified and managed consistent with their relative importance to business objectives and risk strategy. For more information see the IT Management Policy and System Security Plan.
- Business Environment – F2OnSite’s mission, objectives, stakeholders, and activities shall be communicated in an appropriate manner and prioritized. This information shall be used to make Staff aware of cybersecurity roles, responsibilities, and risk management decisions. For more information see the Business Impact Analysis, IT Governance Policy, and Securing Information Systems Policy.
- Governance – policies, procedures, and processes shall be used to implement, manage, and monitor F2OnSite’s regulatory, legal, risk, environmental, and operational requirements. Requirements and cybersecurity risk shall be communicated to the appropriate Staff and Executive Management. For more information see the IT Governance Policy.
- Risk Assessment – Staff shall understand the cybersecurity risk to F2OnSite operations, assets, and to Staff. For more information see the Risk Assessment Policy.
- Risk Management Strategy – F2OnSite’s priorities, constraints, risk tolerances, and assumptions shall be established and used to support operational risk decisions. For more information see the Risk Management Policy.

Protect. F2OnSite Staff shall develop and implement appropriate safeguards to limit or contain the impact of a potential cybersecurity event and ensure the delivery of critical services. Major categories include:

- Access Control – Access to assets and associated facilities shall be limited to authorized users, processes, or devices, and to authorized activities and transactions. For more information see the Identification and Authentication Policy, Logical Access Controls Policy, Network Access Policy, Password Policy, Remote Access Policy, User Privilege Policy, and Wireless Access Policy.
- Awareness and Training – F2OnSite’s Staff shall be provided cybersecurity awareness education and adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. For more information see the Security Awareness and Training Policy and Security Awareness and Training Plan.

- Data Security – Information Resources shall be managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. For more information see the Account Management Policy, Asset Management Policy, Data Classification Policy, Electronic Disposal Policy, and Network Access Policy.
- Information Protection Processes and Procedures – Security policies, processes, and procedures shall be maintained and used to manage protection of Information Resources. For more information see the Security Policy and System Security Plan.
- Maintenance – Maintenance and repairs of Information Resources shall be performed consistent with F2OnSite's policies and procedures. For more information see the Hardware and Software Maintenance Policy.
- Protective Technology – technical security solutions shall be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. For more information see the Anti-malware Policy, Electronic Data Retention Policy, Encryption Policy, Firewall Policy, Patch Management Policy, Quality Assurance Policy, Software Development Policy, System Update Policy, and VPN Policy.

Detect. F2OnSite Staff shall develop and implement the appropriate activities to identify in a timely manner the occurrence of a cybersecurity event. Major categories include:

- Anomalies and Events – activity, and its potential impact, shall be detected in a timely manner. For more information see the Identity Theft Protection Policy, Incident Response Policy, and Logging Policy.
- Security Continuous Monitoring – Information Resources shall be monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. For more information see the Security Monitoring Policy.
- Detection Processes – detection processes and procedures shall be maintained and tested to ensure timely and adequate awareness of events. For more information see the Incident Response Policy.

Respond. F2OnSite Staff shall develop and implement the appropriate activities to take action and contain the impact of a detected cybersecurity event.

- Response Planning – response processes and procedures shall ensure a timely response to detected cybersecurity events. For more information see the Security Monitoring Policy and Incident Response Plan.
- Communications – response activities shall be coordinated with internal and external stakeholders, as appropriate, to include external support from law

enforcement agencies. For more information see the Incident Response Plan and Reporting Violations Policy.

- Analysis – analysis shall be conducted to ensure adequate response and support recovery activities. For more information see the Incident Response Policy and Incident Response Plan.
- Mitigation – Activities shall be performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. For more information see the Incident Response Policy and Incident Response Plan.
- Improvements – response activities shall be enhanced by incorporating lessons learned from current and previous detection/response activities. For more information see the Incident Response Policy and Incident Response Plan.

Recover. F2OnSite Staff shall develop and implement the appropriate activities (e.g. redundancy, failover, etc.) to allow operations to continue and to restore any capabilities or services that were impaired due to a cybersecurity event. Timely recovery to normal operations reduces the impact of a cybersecurity event.

- Recovery Planning – recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. For more information see the Business Continuity Policy, Business Impact Analysis, Business Resumption Plan, Department Continuity of Operations Plan, and IS Disaster Recovery Plan.
- Improvements – recovery planning and processes shall be enhanced by incorporating lessons learned into future activities. For more information see the Business Continuity Policy
- Communications – restoration activities shall be coordinated with internal and external entities. Such entities to include Executive Management, resource owners, Internet Service Providers, etc. For more information see the Business Continuity Communications Plan, Business Continuity Plan, and Business Continuity Policy.

B. CYBERSECURITY FRAMEWORK IMPLEMENTATION

On an annual basis the Chief Security Officer (MGMT) shall evaluate how F2OnSite views cybersecurity risk as well as the processes in place to manage that risk. The evaluation will include cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization's overall risk management practices.

Cybersecurity best practices have identified four cybersecurity framework implementation tiers:

1. Partial. Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad-hoc and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization may not have the processes in place to participate in coordination or collaboration with other entities.
2. Informed. There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis. The organization has not formalized its capabilities to interact and share information externally.
3. Repeatable. The organization's risk management practices are formally approved and expressed as policies. Organizational cybersecurity practices are regularly updated based on the application of risk management processes, changes in business/mission requirements, and a changing threat and technology landscape. There is an organization-wide approach to manage cybersecurity risk. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization understands its dependencies and partners and receives information from these partners that enables collaboration and management decisions within the organization in response to events.
4. Adaptive. The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks. The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

The MGMT's evaluation should identify F2OnSite's current tier level as well as determine if a progression to a higher tier would cost effectively reduce cybersecurity risk.

C. CYBERSECURITY FRAMEWORK PROFILE

The MGMT shall implement and maintain a cybersecurity framework profile that aligns the functions and categories identified in with F2OnSite's business requirements, risk tolerance, and resources of the organization. The profile establishes a prioritized risk management roadmap that reduces cybersecurity risk, is aligned with F2OnSite's goals and objectives, helps meet compliance and regulatory requirements, and is aligned with cybersecurity best practices.

When possible, the MGMT shall establish two cybersecurity framework profiles, one that describes the Current Profile state and another that defines the desired Target Profile state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The MGMT shall perform a comparison of the two profiles, the Current Profile and Target Profile, to reveal gaps to be addressed to meet cybersecurity risk management objectives. The MGMT shall prepare a prioritized action plan to address these gaps.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members that have a responsibility to manage risks related to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 24, 25, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(i), 164.314(a)(2)(i)
ISO 27001 5.2, A.6.1
NIST SP 800-37 2.2, 3.4
NIST SP 800-53 CA-1, PL-1, RA-1, SI-1
NIST Cybersecurity Framework All sections ID.XX, PR.XX, DE.XX, RS.XX, RS.XX, RC.XX
PCI 12.1

CYBERSECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Since all Information Systems rely on operating systems and networks to function, those areas are often targeted for attack and are the main sources of many security vulnerabilities.

II. Purpose

Cybersecurity is the use of various technologies and processes to protect networks, computers, programs, and data. Cybersecurity ensures that F2OnSite's Information Systems are protected by security measures that prevent attacks, damage, or unauthorized access.

III. Scope

This policy applies to all F2OnSite Staff responsible for the security of F2OnSite's Information Resources.

IV. Policy

Cybersecurity helps to maintain an environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, and privacy.

The Chief Security Officer (MGMT) shall establish a risk-based framework core consisting of cybersecurity activities, outcomes, and references that provide guidance for developing individual organizational profiles. The MGMT shall:

- Prioritize and scope. Identify organization objectives and priorities and determine the scope of systems and assets that support the selected business line or process.
- Orient. Identify Information Systems and assets, regulatory requirements, and overall risk approach, identify threats to, and vulnerabilities of, those systems and assets.
- Current Profile. Identify categories, subcategories, and outcomes achieved.

- Risk assessment. Identify the likelihood of a cybersecurity event and the impact on the organization. Consider emerging risks.
- Target Profile. Create a Target Profile focusing on categories, subcategories, and desired cybersecurity outcomes.
- Determine, Analyze, and Prioritize Gaps. Compare the Current Profile and the Target Profile to determine gaps and create a prioritized action plan to address those gaps.
- Implement Action Plan. Determine actions to take and monitor against the Target Profile.

The MGMT shall consider how the cybersecurity program might incorporate privacy principles such as:

- Individual consent to the use of personal information
- Collecting the minimum amount of personal information
- Controls over the use and disclosure of personal information
- Use and retention of personal information related to a cybersecurity incident
- Transparency for certain cybersecurity activities
- Accountability and auditing

A. FUNCTIONS

The MGMT shall identify five concurrent and continuous functions:

- Identify. To better align security with the organization, the MGMT shall understand the business, resources, and cybersecurity risks. Major categories (e.g. Asset Management, Governance, and Risk Management) shall be identified to assist in this effort.
- Protect. The MGMT shall ensure that appropriate safeguards are implemented. Major categories (e.g. Access Control, Security Awareness and Training, Data Security, and Maintenance) shall be identified to protect F2OnSite's Information Systems.
- Detect. The MGMT shall identify cybersecurity events. Major categories shall include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.
- Respond. The MGMT shall identify actions regarding a detected event. Major categories include Response Planning, Communications, Analysis, Mitigation, and Improvements.
- Recover. The MGMT shall ensure F2OnSite's Information Systems maintain resilience and restore capabilities. Major categories include Recovery Planning, Improvements, and Communications. See the Resilience Policy for more information.

B. IMPLEMENTATION TIERS

The MGMT shall identify how F2OnSite views cybersecurity risk and the processes in place to manage that risk. The MGMT shall identify implementation tiers that vary from Partial (Tier 1) to Adaptive (Tier 4). The MGMT shall identify F2OnSite's current implementation tier according to the following criteria:

- Tier 1: Partial implementation. Examples of partial implementation include risk management is not formalized, ad-hoc approach to security, limited awareness of cybersecurity risk, and no collaboration with other entities regarding cybersecurity events.
- Tier 2: Risk Informed. Examples of risk informed include management approves risk management, no wide management of cybersecurity risk, and no capabilities to share info externally.
- Tier 3: Repeatable. Examples of a repeatable implementation include risk management policies, organization-wide management of cybersecurity risk, and F2OnSite receives information from partners that enables risk-based decisions.
- Tier 4: Adaptive. Examples of an adaptive implementation include the ability to adapt security based on lessons learned, predictive indicators, risk management is part of the organization's

culture, information is shared by and with other entities before an event occurs, and continuous awareness of activities on systems/networks.

C. PROFILES

A Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables F2OnSite to establish a roadmap for reducing cybersecurity risk that is aligned with organizational goals, considers legal/regulatory requirements, industry best practices, and reflects risk management priorities.

Profiles help F2OnSite align its cybersecurity activities with its business requirements, risk tolerances, and resources. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile with a “Target” Profile.

The MGMT shall compare the Current Profile with a proposed Target Profile to identify gaps to be addressed to meet cybersecurity risk management objectives.

D. CYBERSECURITY FRAMEWORK

The MGMT shall develop a comprehensive framework that includes Functions (Identify, Protect, Detect, Respond, and Recover), appropriate categories, subcategories, and applicable informative references. See the Cybersecurity Framework Policy for more information. The following table helps illustrate the relationship of Functions, Categories, Subcategories, and references. Additional examples are available in National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

Function	Category	Subcategory	References
Identify	Asset Management	An inventory exists of the physical devices and systems.	ISO 27001 A.8.1.1-2 NIST SP 800-53 CM-8
		Software platforms and applications are inventoried.	ISO 27001 A.8.1.1-2 NIST SP 800-53 CM-8
		Communications and data flows are mapped.	ISO 27001 A.13.2.1 NIST SP 800-53 AC-4, CA-3, CA-9
		External information systems are identified and documented.	ISO 27001 A.8.2.1 NIST SP 800-53 AC-20, SA-9
			ISO 27001 A.8.2.1

		Information Systems are prioritized based upon their classification, criticality, and business value	NIST SP 800-53 CP-2, RA-2, SA-14

E. POLICIES

The MGMT and Chief Risk Officer (CRO) shall ensure that F2OnSite's risks are properly managed and mitigated to the extent possible. The MGMT and CRO shall oversee the implementation and maintenance of formal policies that govern Information Resources.

Desired Security Control	Required Policy/Plan
Governance Leadership Context	Context and Alignment Policy Ethics Policy Health Safety Policy IT Governance Policy Mergers and Acquisitions Policy Terms and Definitions Policy
Information Security	Privacy Policy Securing Information Systems Policy Security Controls Review Policy
Planning Risk Management	Business Impact Analysis Cybersecurity Policy Cybersecurity Framework Policy Risk Assessment Policy Risk Management Policy
Policies and Procedures	Security Policy Security Policy Introduction System Security Plan
Organization	Audit Policy IT Management Policy Non-Disclosure Agreement Outsourcing Policy Staffing Policy Security Self Assessment Policy
Asset Management	Access Control Policy Asset Management Policy Configuration Management Plan Configuration Management Policy Data Classification Policy Software Licensing Policy
Human Resources	Acceptable Use Policy

Communication	Audit Policy Security Awareness and Training Plan Security Awareness and Training Policy Staffing Policy Social Networking Policy Third Party Service Providers Policy
Physical Environmental	Facility Security Plan Personnel Security Policy Physical Access Policy Physical Security Policy
Operation Support	Account Management Policy Anti-Malware Policy Backup Plan Backup Policy Bluetooth Policy Capacity and Utilization Policy Data Analytics Policy Data Integrity Policy Data Marking Policy Data Privacy Policy Disposal Policy Documentation Policy Domain Controller Policy Domain Name System Policy E-commerce Policy E-mail Policy Firewall Policy Guess Access Policy Internet Connection Policy Intrusion Detection Policy Logging Policy Mass Communication Policy Network Address Policy Network Configuration Policy Network Documentation Policy Network Security Policy Problem Management Policy Ransomware Policy Removable Media Policy Router Security Policy Security Monitoring Policy Server Hardening Policy Vendor Access Policy Workstation Hardening Policy

	Workstation Security Policy
Access Control	Access Control Policy Admin Special Access Policy Bring Your Own Device Policy and Technology Guest Access Policy Identification and Authentication Logical Access Controls Policy Mobile Device Policy Password Policy Portable Computing Policy Remote Access Policy Securing Information Systems Policy Securing Sensitive Information Policy Smartphone Policy System Update Policy User Privilege Policy Wearable Computing Device Policy Web Policy Wireless Access Policy
Acquisition Development Maintenance	Acquisition and Procurement Policy Application Implementation Policy Approved Application Policy Audit Trails Policy Change Management Policy Encryption Policy Green Computing Policy Hardware and Software Maintenance Patch Management Policy Production Input Output Controls Policy Quality Assurance Policy Secure Development Lifecycle Policy Server Certificates Policy Software Development Policy VPN Policy Web Site Policy
Incident Management	Identity Theft Protection Policy Incident Response Policy Incident Response Plan Reporting Violations Policy
Business Continuity Disaster Recovery	Business Continuity Plan Business Continuity Policy Business Resumption Plan Continuity Communications Plan

	Department Continuity of Operations Plan IS Disaster Recovery Plan Resilience Policy
Compliance Performance Evaluation	Business Associates Agreement Certification and Accreditation Policy Compliance Policy Data Retention Policy GDPR EU Privacy and Data Protection Policy HIPAA and HITECH Policy HITRUST Policy PCI Policy Security Controls Review Policy Software Licensing Policy System and Organization Controls SOC2 Policy Vulnerability and Penetration Testing Policy

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information and physical security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO11.01-02, APO11.04-05, BAI02.04, BAI03.06, BAI03.08, BAI07.03, BAI07.05

GDPR Article 25

HIPAA 164.308(a)(2)

ISO 27001 A.8.1.1-2, A.8.2.1, A.13.2.1

NIST SP 800-37 3.1

NIST SP 800-53 AC-4, AC-20, CA-3, CA-9, CM-8, CP-2, RA-2, SA-9, SA-14

NIST Cybersecurity Framework All sections ID.XX, PR.XX, DE.XX, RS.XX, RS.XX, RC.XX

PCI A3.2.3, PCI Software Security Framework

DATA ANALYTICS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Data analytics helps F2OnSite increase revenues, improve operational efficiencies, optimize marketing campaigns, enhance customer service, respond more quickly to trends, gain a competitive edge in our marketplace, and enhance business performance.

II. Purpose

The purpose of this policy is to provide a foundation for the development and implementation of necessary security controls to protect data according to its value and/or risk. Data that is analyzed may originate from a mix of internal systems and/or external sources. The data may consist of either historical records or new information that has been processed for use in real-time analytics.

III. Scope

This policy applies to all Staff involved in the collection, preparation, use, storage, and disposal of analyzed data.

IV. Policy

A. BACKGROUND

Data analytics refers to techniques and processes used to extract and categorize data for the purpose of identifying and analyzing data and patterns. Data analytics involves the discovery, interpretation, and communication of meaningful patterns in data. Data analytics may include data mining, which can include sorting through large volumes of data to identify trends, patterns, and data relationships. Predictive analytics seeks to predict behavior and future events.

Software analytic applications, a type of business intelligence software, use historical data to provide information and tools that allow management to make informed

business decisions. Self-service business intelligence tools allow users to create and run their own ad hoc queries and reports.

Data analytics typically involves the following phases:

- Data collection (data ingestion). Identify information needed and resources to collect or assemble the data.
- Data preparation. Perform data profiling and cleansing to ensure the data is in an appropriate format, type, length, etc. Duplicate records are eliminated and data governance policies are applied to ensure that the data adheres to required standards. Issues involving large numbers of data records are addressed.
- Data analytics. Predictive modeling and analytics software and programming languages such as Python, Scala, R and SQL may be used. On large data volumes, the software may initially run against a subset of the data to ensure the data and model are working as desired.
- Data communications. The results generated by analytical models are communicated to users and management.

A data lake is data stored in its natural or raw format. A data lake may include raw copies of data as well as transformed data used for reporting, visualization, analytics, machine learning, etc. Data lakes may include unstructured data (e.g. documents, e-mail messages, PDF files, etc.) in natural format, structured data from relational databases, as well as binary data such as images, audio, and video. Cloud storage services such as Microsoft Azure Data Lake and Amazon S3 or a distributed file system such as Apache Hadoop may be used.

Data virtualization allows an application to retrieve and manipulate data without knowing technical details (e.g. formatting, location) about the data.

Big data applications collect, manage, and process large volumes of data that are typically beyond the ability of commonly used software. Big data has the following characteristics:

- Volume – large amount of data.
- Variety – type and nature of the data
- Velocity – speed at which the data is generated and processed
- Veracity – data quality and value

B. SECURITY CONTROLS

The Risk Management Officer (RMO) shall ensure risks are properly identified and managed through a three-step process (for more information see the Risk Management Policy):

- Risk Assessment – Identify assets, threats to the assets, and vulnerabilities that exist as a result of the threats.
- Risk Analysis – For each risk, identify the likelihood and impact on our organization.
- Risk Treatment Plan – Develop controls and other safeguards designed to mitigate, eliminate, or transfer risks. It is important to treat risks in a cost effective and efficient manner.

The Chief Security Officer (MGMT) shall ensure adequate safeguards are in place to ensure the security of Sensitive Information and Information Systems. Safeguards shall protect against electronic threats as well as unauthorized access, disclosure, copying, use or modification of systems and data. Data collected and processed shall be limited to the amount and type of information specifically required for an identified purpose. For more information on applicable security controls and requirements see:

- Access Control Policy
- Anti-malware Policy
- Application Implementation Policy
- Approved Application Policy
- Backup Policy
- Capacity and Utilization Policy
- Configuration Management Policy
- Data Classification Policy
- Data Privacy Policy
- Encryption Policy
- Firewall Policy
- Logging Policy
- Network Security Policy
- Physical Access Policy
- Privacy Policy
- Retention Policy
- Security Controls Review Policy
- Software Development Policy
- Third Party Service Providers Policy
- User Privilege Policy

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads, the Risk Management Officer, and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO10.05, APO12.02, APO13.07, APO14.10, BAI01.03, BAI04.05

GDPR Article 9, 10, 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(3)(ii)(B), 164.308(b)(4)

ISO 27001 6.1.3, 9.1, A.8.2.1, A.9.1.2, A.9.4.1, A.12.1.3, A.12.2.1, A.12.4.1, A.12.6.2, A.13.2

NIST SP 800-37 3.3, 3.4, 3.5

NIST SP 800-53 AC-1, AC-3, AC-24, PM-29, RA-2, SC-13, CP-2

NIST Cybersecurity Framework ID.RA-6, PR.AC-4, PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-5

PCI 3.1, 7.1, 12.2

DATA CLASSIFICATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All F2OnSite data, whether electronic or printed, should be classified. The data owner, who is responsible for Data Classification, should consult with legal counsel on the classification of data as Public, Sensitive, or Confidential. Consistent use of data classification reinforces with users the expected level of protection of F2OnSite data assets in accordance with F2OnSite security policies.

II. Purpose

The purpose of this policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Data shall be classified as listed below.

Public. Information intended or required for public release. Disclosure of such information does not adversely impact F2OnSite's business operations, financial well being, or our image and reputation.

Sensitive. Sensitive data that requires additional levels of protection. Examples of sensitive data include but are not limited to:

- Operational information
- Personnel records
- Information security procedures
- Research
- Internal communications
- Log records (firewall logs, audit trails, etc.).

Confidential. Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements. Examples of "Confidential" data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Employment Records
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets
- Medical Records

Controlled Unclassified Information (CUI). Information, excluding Classified Information, that requires safeguarding or dissemination controls required by laws, regulations, or Government-wide policies.

Access to authentication data shall be restricted to authorized personnel through the use of encryption, file access controls, or both encryption and file access controls.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO14.01-02, APO14.07, APO14.10, BAI02.05

GDPR Article 9, 10

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)

ISO 27001 A.8.2

NIST SP 800-37 P-10

NIST SP 800-53 PM-29, RA-2

NIST Cybersecurity Framework ID.AM-2-3, ID.AM-5

PCI 3.1, 12.2

DATA INTEGRITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Controls and safeguards are needed to protect the integrity of electronic data that is stored, accessed, or transmitted using Information Resources.

II. Purpose

This policy ensures the integrity of F2OnSite's data. Data should be protected from unauthorized alteration or destruction.

III. Scope

Data integrity is an enterprise-wide activity that applies to all F2OnSite Departments. This policy applies to all F2OnSite Staff that store, access, or transmit electronic data.

IV. Policy

Each department shall protect electronically stored, accessed, or transmitted data.

Each Department shall implement processes that:

- Protect data from unauthorized alteration or destruction.
- Monitor access to data to ensure that it has not been altered or destroyed due to unauthorized activity.
- Issue alerts if the data has been altered or destroyed in an unauthorized manner. Upon such alerts, implement corrective action procedures to ensure data is restored and implement controls to ensure data is protected and cannot be altered in an unauthorized manner in the future.

The processes and technologies instituted by a department must achieve a level of protection sufficient to ensure data integrity. Each Department shall provide additional protections as needed when stricter requirements apply.

When designing or implementing security controls, the departments should ensure that they are in compliance with this policy.

On an annual basis, each Department shall submit a list of administrative, physical, and technical data integrity controls to the Chief Security Officer (MGMT). The MGMT will review the controls to ensure they are appropriate, sufficient, and effective at ensuring data integrity.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for Information System security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10
GDPR Article 25, 30, 32
HIPAA 164.312(c)(2), 164.312(e)(2)(i)
ISO 27001 A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.1.4, A.18.2.2
NIST SP 800-37 P-14
NIST SP 800-53 PM-25, SC-8, SI-1
NIST Cybersecurity Framework PR.AC-5, PR.DS-6, PR.DS-8, DE.DP-2, RS.RP-1
PCI 3.6.5, 4.1, 6.4.6, 10.5, 10.6.1, 11.5, 12.10.5

DATA MARKING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's Information Systems contain sensitive information that must be protected from unauthorized access throughout all phases of the information lifecycle. By properly marking data, F2OnSite helps ensure that it can be properly protected.

II. Purpose

Failure to protect sensitive information can lead to fraud, waste, abuse, and other negative outcomes that ultimately damage both the business and our relationships with customers, suppliers, and other critical entities. This policy also helps manage risks related to legal and compliance requirements and our ability to continue business operations.

III. Scope

This policy applies to all F2OnSite Staff who use Information Resources.

IV. Policy

Staff in both IT and business roles shall use physical and technical mechanisms to ensure secure handling, transfer, and storage of data via electronic and paper documents, printouts, backup media, electronic storage, and removable media. Staff must also consider sensitive information that may be saved on media and equipment slated for disposal.

All hardware, output, and media that contain Sensitive Information shall be clearly marked.

A. GENERAL

All Sensitive Information and material shall be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal Sensitive Information, the period of time protection is required, and any other notations required for protection of the information.

- **Hardware Components.** All components of an information system, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the Information System. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen.
- **Hard Copy Output and Removable Media.** Output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human-readable, external markings to the level of the information.
- **Unclassified Media.** In the approved areas where classified and non-classified information are processed on collocated information systems, unclassified media shall be so marked.

B. IDENTIFICATION MARKINGS

All classified material shall be marked to show the name and address of the party responsible for its preparation, and the date of preparation.

- **Files, Folders, or Groups of Documents.** Files, folders, binders, envelopes, and other items containing Sensitive Information, when not in secure storage, shall be conspicuously marked.
- **E-mail and other Electronic Messages.** Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text. A "Derived From" line is required on messages. Certain departments may also require that messages contain a "Classified By" and a "Reason Classified" line in order to identify the derivative classifier and the specific reason for classification. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The last line of text of the message shall include the declassification instructions.

- **Derivative.** A new document or copy shall be marked with the same classification markings as applied to the information or document from which the new document or copy was prepared.
- **Not classified.** If the information was not previously classified, the information shall be protected as though classified at the appropriate level and submitted to the appropriate department for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used and shall conspicuously appear on the material:

CLASSIFICATION DETERMINATION PENDING
Protect as though classified as Confidential

Electronic output to be released outside the security boundary shall be verified by a comprehensive review (e.g. in human readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) shall be examined for content using the appropriate software application. Random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

C. INADVERTENT RELEASE

The following steps shall be performed if Sensitive Information is inadvertently distributed outside the company without the proper classification assigned to it, or without any markings to identify the material as classified:

- Determine whether all holders of the material are cleared and authorized access to it.
- Determine whether control of the material has been lost.
- If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to management.
- Media shall be protected until an appropriate classification review has been conducted. An appropriate sensitivity and classification review shall be performed on human readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

D. RESPONSIBILITIES

The Chief Security Officer shall be responsible for approving documented processes that:

- Ensure security during reproduction of sensitive data files.
- Ensure security during receipt or sending of media that contains sensitive data.
- Log transmittal and transport records related to media that contains sensitive data.
- Investigate and resolve any discrepancies between internal records and transmittal and transport logs.
- Defines in the security plan disposition procedures for media no longer used to process or store sensitive information.

Department heads shall:

- Train employees on security requirements for equipment and media containing sensitive information.
- Monitor employee activities to ensure compliance with security policies and procedures.
- Work with System Administrators to ensure that only authorized software runs on automated information systems.
- Approve, as needed, reproduction of sensitive data files.
- Sign for, or delegate authority to sign for, receipt of registered, certified, or express mail which can contains sensitive data.
- Review transmittal logs and transport records on a weekly basis to account for all removable media that contains sensitive information.
- Investigate and resolve any discrepancies between internal records and transmittal and transport logs.
- Work with the Chief Security Officer to define disposition procedures for media no longer used to process or store sensitive information.
- Establish and communicate requirements for protecting systems and data
- Ensure that sensitive data is not stored on personal computers.
- Track sensitive data from creation through destruction.

Staff shall:

- Adhere to security requirements for the protection of sensitive data and systems.
- Appropriately identify, date, and mark sensitive information they are responsible for originating, producing, or processing.
- Ensure that media containing sensitive data is appropriately labeled.
- Ensure that media containing sensitive data is stored in secure locations and/or containers.
- Ensure that media does not contain both sensitive and non-sensitive information.
- Ensure that sensitive information is not left on output devices after printing.
- Sign for all data sent, received, or transported.

- Shred sensitive printed documents and follow secure disposition procedures for media.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10
GDPR Article 32
HIPAA 164.308(a)(7)(ii)(E)
ISO 27001 A.8.2.2, A.8.2.3, A.8.3
NIST SP 800-37 3.2, 3.3
NIST SP 800-53 AC-16, MP-3, PE-22
NIST Cybersecurity Framework ID.AM-2, ID.AM-3, PR.PT-2, DE.DP-2, DE.CM-2
PCI 9.9.2

DATA PRIVACY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's computer systems and related devices collect and record activity for business purposes. This information should not be disclosed to unauthorized individuals.

II. Purpose

This policy establishes general privacy requirements for information automatically generated by computer systems and network devices, including systems and devices involved in the transmission and storage of voice data. The policy further delimits the conditions under which network data may be disclosed.

III. Scope

This policy applies to all F2OnSite Staff who use Information Resources.

IV. Policy

A. NETWORK DATA

In the course of normal network operations, computer systems, voice systems, access control systems, and network devices may automatically generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (Network Data).

It is the general policy of F2OnSite to treat Network Data as private. This information may be obtained, stored, and reported for legitimate business purposes but shall not be exposed to unauthorized individuals except as specifically listed below.

B. EXCEPTIONS

Network Data may be exposed or disclosed under the circumstances listed below.

To maintain the integrity and availability of network operations. Network Data may intentionally or inadvertently expose Information Resources stored on networked machines or transmitted through the network in the following situations:

- Network performance monitoring or troubleshooting.
- Moving data through the network via automated store-and-forward systems.
- Copying, archiving, or otherwise preserving portions of messages transmitted over the network in the course of routine network maintenance activities.

In the event that messages or data files within the network indicate the presence of activities that violate internal policies or law.

In the event of recognized network security threats. F2OnSite reserves the right to investigate and remediate possible network security threats, including by means of capture, logging, and examination of files, communications, and other traffic and transmissions over or on the network.

In response to a court order.

In the event of a legitimate health or safety emergency.

In pursuit of reasonable business interests, such as fulfillment of partnership agreements.

C. REQUESTS FOR NETWORK DATA

All requests to retrieve and share Network Data must be submitted to the IT Department and must be approved by the appropriate Department head. Such requests shall include:

- Name and role of the requestor.
- Reason for the request, in accordance with the principles set forth in this policy.
- Intended use of the requested data.

Any network data intentionally shared with third parties must be sanitized to preserve the anonymity of network users.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)

ISO 27001 A.8.2

NIST SP 800-37 P-10

NIST SP 800-53 PM-29, RA-2

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RM-1, DE.DP-2

PCI 3.1, 12.2

DATA RETENTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite must balance our legal obligations and need to retain information for business purposes against the cost of storing and securing such information.

II. Purpose

This policy helps manage risks related to legal and compliance requirements and our ability to continue business operations.

III. Scope

This policy applies to all Staff that have access or and data retention responsibilities for F2OnSite's Information Resources.

IV. Policy

A. RESPONSIBILITIES

F2OnSite's Legal Department shall establish enterprise-wide retention procedures for the organization. In establishing F2OnSite's retention procedures, the Legal Department shall consider legal and compliance requirements, litigation needs, business processes, privacy concerns, and the cost of retaining information.

The Legal Department is responsible for preparing and maintaining a comprehensive data retention, archiving, and destruction schedule (Retention Schedule). The Retention Schedule will consider active and inactive electronic information including data held in servers, databases, storage arrays, backup media, important workstations, e-mail, log files, video cameras, and other types of electronic storage devices.

When establishing retention periods, the Legal Department will perform the following steps:

- Determine applicable legal or compliance requirements.

- Determine, with the help of F2OnSite Departments, the collection, storage, archiving, and use of electronically stored data.
- Identify other internal or external Departments or business entities that collect, store, archive, or use electronically stored information.
- Establish retention periods for electronically stored information based on information obtained in the prior steps.

Each F2OnSite department will develop procedures and documentation that implement and maintain the retention requirements as outlined in the Retention Schedule. The specific procedures implemented by each Department will specify the retention time, archival rules, data formats, and the permissible means of storage, access, and encryption (if any).

B. RETENTION REQUIREMENTS

The Chief Security Officer (MGMT) shall:

- Implement data retention and disposal guidelines that limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements.
- Ensure quarterly automatic or manual processes exist for the secure deletion of data when no longer needed.
- Establish specific retention requirements for sensitive data.

Different types of data require different retention periods. In addition to describing how long various types of information must be maintained, department retention procedures must specify:

- Steps used to archive the information.
- The appropriate destruction of electronically stored information after the identified retention period. Such steps shall adhere to the requirements outlined in the Disposal Policy.
- Procedures for handling electronically stored information when under litigation.

Each department may have unique data retention requirements that must be communicated to the Legal Department. Such requirements may include contractual obligations with customers or business contacts or data retention requirements to maintain business operations. In some instances, departments may need to retain electronically stored information for a historical archive.

To meet regulatory and organizational requirements, the Legal Department:

- Will identify retention periods for log files and audit trails.
- May choose to alter e-mail retention requirements specified in the E-mail Policy.

During the appropriate retention period, archived data must be retrievable.

- As new software and/or hardware is implemented, the IT Department shall ensure that new systems can read legacy data. This may require old data be converted to new formats.
- Data that is encrypted must be retrievable. The IT Department shall implement key management procedures that ensure encrypted data can be decrypted when needed.

C. RETENTION RESOURCES

When establishing retention periods, the Legal Department may rely on one or more of the following legislative requirements.

Code of Federal Regulations - organizations must retain compliance evidence for not less than 2 years in a form that is capable of accurately retaining and reproducing information. If the organization is being investigated, it must retain the records pertaining to the action until final disposition, unless disposal is allowed by court order. [229.21(g), 12 CFR Part 229 Availability of Funds and Collection (Check Clearing for the 21st Century)]

Energy - retain all records and the supporting technical documentation required to satisfy this section's requirements until the license for which the records were developed has been terminated by the Nuclear Regulatory Commission. Superseded portions of records must be retained for at least 3 years after being superseded, unless the Commission has specified otherwise. [73.54(h), 10 CFR Part 73.54, Protection of digital computer and communication systems and networks]

Healthcare

- Records shall be kept for a time period equal to the design and expected life of the device, but not less than 2 years from the commercial distribution release date. [820.180(b), 21 CFR Part 820, Subchapter H - Medical Devices, Part 820 Quality System Regulation]
- Required documentation shall be kept for 6 years from the creation date or the date it was last in effect, whichever is later. [164.316(b)(2)(i), 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards, Final Rule]
- Eligible hospitals, eligible professionals (EPs), and critical access hospitals (CAHs) must keep documentation that supports the demonstration of meaningful use for 6 years. [495.8(c)(2), 422.504(d), 495.8(c)(2), 42 CFR Parts 412, 413, 422 et al., Medicare and Medicaid Programs; Electronic Health Record Incentive Program, Final Rule]
- Documentation required by 164.530(j)(1) must be retained for 6 years from the creation date or the date it was last in effect, whichever is later. [164.530(j)(2), 45

CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information, Final Rule]

- The Records Officer must ensure signed forms and related documentation, for personnel departures, are kept in a centralized file for at least 10 years in the Records Management or Personnel office. [Department of Health and Human Services Records Management Procedures Manual, Version 1.0 Final Draft]

National Association of Securities Dealers - keep all such documents for a period of not less than 5 years, the first 2 years in an easily accessible place, subject to the destruction and disposition provisions of Rule 17a-6. [240.17a-6(b), 17 CFR Part 240.17a-1, Recordkeeping rule for securities exchanges]

Payment Card Industry (PCI)

- The organization must ensure audit trails are retained for at least 1 year and must have the last 3 months available for immediate analysis (i.e. on-line, archived, or restorable from backup). [10.7, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures]
- Examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least 1 year with the most recent 3 months available. [10.7.a Testing Procedures, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures]
- Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data storage: Limit data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements, specific retention requirements for cardholder data, processes for secure deletion of data when no longer needed, and a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. [3.1 Protect Stored Cardholder Data, Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures]

Sarbanes Oxley - The organization must prepare and maintain audit work papers and other information for not less than 7 years. [103(a)(2)(A)(i), 1520(a)(2), The Sarbanes-Oxley Act of 2002 (SOX)]

Tax - Records of the requests by or to the organization for Federal Tax Information must be maintained for 5 years. [5.01(1), IRS Revenue Procedure: Record retention: automatic data processing, 98-25]

U.S. Federal Security - All required records must be kept for a period of 5 years. [762.6(a), US Export Administration Regulations Database]

Various State Laws - When a breach investigation concludes that the breach has not and will not likely result in harm to any individuals, the organization must document the non-notification requirement in writing and maintain the documentation for 5 years.

[45.48.010(c), Alaska Personal Information Protection Act, Chapter 48]

[817.5681(10), Florida Statute 817.5681 Breach of security concerning confidential personal information in third-party possession]

[715C.2.6, Iowa Code Annotated 715C Personal Information Security Breach Protection]

[14-3504(b)(4), Maryland Code of Commercial Law Subtitle 35. Maryland Personal Information Protection Act 14-3501 thru 14-3508] (3 years)

[407.1500.2(5), Missouri Revised Statutes Chapter 407 Merchandising Practices 407.1500]

[56:8-163.a, New Jersey Permanent Statutes Title 56 Security of Personal Information]

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO12.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 5

HIPAA 164.316(b)(2)(i)

ISO 27001 A.8.2, A.8.3.2

NIST SP 800-37 3.2, 3.7

NIST SP 800-53 AC-16, AT-4, AU-11, MP-6, SA-19(3), SI-12

NIST Cybersecurity Framework ID.AM-2, ID.AM-4, ID.GV-3, PR.IP-6

PCI 3.1, 10.7

DATABASE SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Databases and the data that they contain must have proper security controls that protect against loss of data or unauthorized access or alteration.

II. Purpose

The purpose of this policy is to establish the rules for the access and protection of databases. These rules are necessary to preserve the integrity, availability and confidentiality of F2OnSite's databases and data.

III. Scope

This policy applies to F2OnSite Staff who perform network administration, database administration (DBA), or web development duties.

IV. Policy

A. Access

The Chief Security Officer (MGMT) shall ensure Staff must receive prior written authorization before they are permitted to access databases and data.

B. Security Protection

The MGMT shall ensure that appropriate security mechanisms are implemented to protect databases from unauthorized access or alteration. Examples of such security mechanisms include:

- Access control policies including password policies
- Information Systems Access Request Form
- Network segmentation
- Network firewalls and web application firewalls
- Router Access Control Lists (ACL)

Software applications that access F2OnSite databases must use proper coding and security techniques:

- Database user names and passwords (credentials) shall only be accessible by authorized persons, programs, and processes.
- Credentials must adhere to specifications listed in F2OnSite's Password Policy.
- Access to databases shall be granted only after authentication of proper credentials.
- Database access credentials must not be stored in readable clear text format.
- To reduce the likelihood of unauthorized access, source code credentials must be stored in a separate source file. The credentials file may contain user names, passwords, and any code needed to access the credentials.
- Credentials stored in an external file shall be read from the file immediately prior to use and, immediately after authentication, the memory containing the credentials shall be cleared or released.
- Database authentication may occur programmatically as part of the user authentication process on an authentication server.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the MGMT, Network Administrators, Database Administrators (DBAs), and web developers.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.8.1.3, A.9

NIST SP 800-37 3.4

NIST SP 800-53 AC-3, AC-24

NIST Cybersecurity Framework PR.AC-5, PR.AC-7, PR.DS-1, DE.DP-2

PCI 1.1.3, 2.2

DISPOSAL POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite Staff store sensitive information on computer hard drives and other forms of electronic media. As new equipment is obtained and older equipment and media are phased out, sensitive information on the old equipment and media must be properly erased or otherwise made unreadable.

II. Purpose

F2OnSite faces several risks related to the disposal of hard drives and other computer storage media:

- Violation of Software License Agreements - Most software is licensed for use on either a single computer system, to a single person, or to an organization. Usually these licenses are not transferable. Even when the licenses are transferable, there may be specific requirements that must be met, such as possession of the original distribution media, consent of the licensor, or payment of a transfer fee, in order to effect the transfer. Allowing a third party access to licensed software without proper transfer of the license may be a breach of the license agreement, and may subject the state or the recipient of the software to claims for damages.
- Unauthorized Release of Confidential Information - Allowing an unauthorized person access to confidential information can subject F2OnSite and sometimes individual employees, to claims for damages.
- Unauthorized Disclosure of Trade Secrets, Copyrights, and Other Intellectual Property – F2OnSite computer systems develop and store data, programs, designs, techniques, etc., that are or will become valuable assets of the organization as either trade secrets, copyrighted materials, patented inventions, or other intellectual property. Accidental or premature disclosure could mean a loss of secrecy under trade secrets law or constitute a publication under federal copyright law, either of which might result in loss of the asset.

III. Scope

This policy applies to all F2OnSite Staff that have access to Information Resources.

IV. Policy

The Chief Security Officer shall ensure:

- Procedures address the final disposition of sensitive information, hardware, or electronic media.
- Procedures specify the process for making sensitive information unusable and inaccessible. Procedures specify the use of a technology (e.g. software, special hardware, etc.) to make sensitive information unusable, inaccessible, and not able to be reconstructed.
- Procedures specify the personnel authorized to dispose of sensitive information or equipment containing sensitive information. Such procedures may include shredding, incinerating, or pulp of hard copy materials so that sensitive information cannot be reconstructed.

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled. Data can be present on any type of storage device, whether fixed or removable, that contains data and maintains the data after power is removed from the device. Due to the advances in computer forensics, simply deleting the data and formatting the disk will not prevent someone from restoring the data. However, sanitization of the storage media removes the information from the media in such a way that data recovery using common techniques or analysis is prevented.

Any and all computer desktops, laptops, hard drives, and portable media must be given to the IT Department for proper disposal. Paper and hard copy records should be disposed of in a secure manner as authorized by the Chief Security Officer (MGMT). The MGMT's analysis of secure disposal processes should include, but not be limited to, shredders and storage of records in a secure area for an authorized disposal/recycling service.

Overwriting is a software procedure that replaces the data previously stored on magnetic storage media with a predefined set of meaningless data. At a minimum, overwriting should be performed using a character, its complement, then a random character. For confidential information, additional overwriting using different characters is recommended.

Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process.

Unless IT Department Staff can absolutely verify that no personal or confidential information, intellectual property, or licensed software is stored on the hard drive/storage media, the hard drive/storage media shall be sanitized or be removed and physically destroyed.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 5

HIPAA 164.310(d)(2)(i), 164.316(b)(2)(i)

ISO 27001 A.8.3.2

NIST SP 800-37 3.2, 3.7

NIST SP 800-53 MP-6, SA-19(3)

NIST Cybersecurity Framework ID.AM-2, ID.AM-3, ID.GV-3, PR.DS-3, DE.DP-2

PCI 3.1, 3.2

DOCUMENTATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Documentation is important to ensure the continued operation of Information Resources in a reliable, secure, and sound manner.

II. Purpose

This policy establishes the framework for Information Resources documentation.

III. Scope

This policy applies to the IT Department and other departments responsible for acquiring, implementing, and maintaining Information Resources.

IV. Policy

A. RESPONSIBILITIES

The Chief Security Officer shall ensure:

- The organization makes documentation available to those responsible for implementing the procedures to which the documentation pertains.
- The organization reviews documentation periodically, and update as needed, in response to changes affecting the security of sensitive information.
- Operating procedures are documented and made available to all Staff that need them.

Documentation is a mandatory requirement for all of F2OnSite's Information Resources. Such documentation shall be kept up-to-date and be available to authorized personnel. The documentation shall be reviewed annually by a Documentation Analyst to verify it is appropriate, sufficient, and effective at continuing Information Resource availability, confidentiality, and integrity.

The Documentation Analyst shall collect and assemble documentation into an Information Resources Documentation Manual (Manual). The Documentation Analyst shall ensure that the Manual is updated on an annual basis or more frequently if changes occur.

B. NETWORK DOCUMENTATION

Network documentation shall include:

- Documentation on servers and major applications including data owners.
- Network diagrams with the locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
- The various security zones on the network and devices that control access between them.
- Connectivity between all segmented networks.
- All subnets on the network and their relationships including the range of IP addresses on all subnets and netmask information.

Configuration information on all network devices including switches, routers, hubs, and firewalls shall include:

- IP Address
- Netmask
- Default gateway
- DNS server IP addresses for primary and secondary DNS servers

Network connection information shall include the Internet provider, type of connection to the Internet, provider contact information, configuration information, and physical location including building and circuit number.

C. DOCUMENTATION ACCESS

Access to documentation shall be permitted as follows:

- The Documentation Analyst has full access to all Information Resources documentation.
- The IT network and security staff shall have full access to all network documentation.
- The IT network staff shall have the ability to read and modify network documentation.
- The Help Desk staff shall have read access to network documentation.
- Security staff shall have access to read and change security related documentation.

D. DOCUMENTATION REVIEW

The Documentation Analyst shall ensure that Information Resources documentation is kept current by performing an annual review of documentation. The Documentation Analyst will review Help Desk and Incident Response logs to determine whether changes were made to Information Resources. In addition, the Documentation Analyst will review projects related to Information Resources to determine whether the documentation needs to be updated.

E. DOCUMENTATION STORAGE

Information Resource documentation shall be maintained in both written and electronic form and retained through the full life of the Information Resource.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all IT Department personnel and other F2OnSite staff members responsible for acquiring, implementing, and maintaining Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02-03, APO05.05, APO11.09-10, APO12.02, APO12.07, APO13.07, BAI11.09
 GDPR Article 30, 33, 49
 HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E)
 ISO 27001 7.5, 8.1-3, 9.1-3, 10.1, A.8.1.3, A.9.1.1, A.12.1.1, A.14.2.5, A.15.1.1
 NIST SP 800-37
 NIST SP 800-53 All XX-1 controls, SA-5, SA-8, SA-12
 NIST Cybersecurity Framework ID.RA-1, ID.RA-3, PR.PT-1, RS.MI-3
 PCI 1.1.2-3, 1.1.5-6, 1.5, 2.5, 3.5-7, 4.3, 5.4, 6.4.5

DOMAIN CONTROLLER POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's Information systems are critical to the continued operations of essential business processes. Domain Controllers (DC) are an essential component of F2OnSite's network.

II. Purpose

Domain controllers, as well as backup domain controllers, are central to the security of all devices on that network and must be protected. The actions necessary to secure domain controllers are listed in this policy.

III. Scope

This policy applies to all F2OnSite Staff that have access to Information Resources.

IV. Policy

The domain controller function is incompatible with other functions such as web server, mail server, ftp server, or mail client that can increase the risk of compromise to an unacceptable level. As a result, domain controllers shall be established on a dedicated device.

Domain controllers shall have restricted Internet access. In addition, the domain controllers shall have limited communications with specific devices (or an IP range if not practical to individually list the devices) on the F2OnSite network.

Domain controllers shall deny access to unknown machines on the Internet and network using either filtering, firewall, or non-routed network addressing.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for installing, maintaining, and securing domain controllers.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.310(d)(1)

ISO 27001 A.11.2, A.12

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-3, AC-4(2), AC-5, CA-3, SC-2, SC-3, SC-20

NIST Cybersecurity Framework ID.AM-1-2, ID.BE-4, ID.GV-1, ID.RA-1, ID.RM-1, DE.DP-2

PCI 6.1-4, 6.7, 7.1-2, 8.1

DOMAIN NAME SYSTEM POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to protecting its employees, customers, partners and its operations. This policy enables F2OnSite to effectively deliver equipment and services that support company business processes.

II. Purpose

This policy protects F2OnSite's assets and helps ensure our ability to continue business operations.

III. Scope

This policy applies to all F2OnSite Staff that have access to Information Resources.

IV. Policy

The IT Department shall only approve requests for variations on a domain name (whether for a physical server or a virtual server) to major departments or entities. When a request for a domain name which doesn't include a leading "www" is approved, a second domain, which includes the leading "www," will also be generated.

- The preferred format for domain names shall be: entity.ABCCompany.com/department/ or server.ABCCompany.com/department/.
- Names will adequately, appropriately, and uniquely describe the unit/content, while keeping the address as short as possible.
- Domain names shall be all lower case and shall not include spaces or any special characters (e.g. \$, @, &).
- When necessary, domain names shall use a hyphen to separate words.

The appropriate Department Head shall approve the request and forward to a System Administrator. The System Administrator shall review the request for appropriateness

and implement the request if it complies with this policy. System Administrators shall watch for inappropriate words within the address, especially when combining words. Requests that do not meet the requirements stated in this policy shall be forward to the IT Director for resolution.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for installing, maintaining, and securing the network infrastructure.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO03.06-08, APO13.07, APO14.10, DSS04.05
GDPR Article 25
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2)
ISO 27001 A8, A9
NIST SP 800-37 3.1, 3.3
NIST SP 800-53 CM-8, PL-4
NIST Cybersecurity Framework ID.AM-2, ID.AM-5, ID.BE-4, ID.RA-6, ID.SC-1, PR.PT-4
PCI 1.1.5

E-COMMERCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite continues to enhance the way we provide products and services to our customers. As a convenience to our customers and business partners, we now accept electronic payment via credit cards. following guidelines highlight the most critical issue in providing this service, to ensure that the trusted relationship between F2OnSite and its customers is conducted in the most secure, confidential and reliable method possible.

II. Purpose

This policy ensures that the trusted relationship between F2OnSite and its customers is conducted in the most secure, confidential, and reliable method possible.

III. Scope

This policy applies to all F2OnSite Staff that have access to Information Resources.

IV. Policy

F2OnSite Executive Management must review and approve all proposed electronic commerce (e-commerce) solutions. All e-commerce platforms must either be hosted by F2OnSite's IT Department or hosted through a contractual relationship with a third party service provider.

E-commerce solutions will be reviewed based upon the business case, financial impact, technical requirements, and security mechanisms. The associated startup and recurring costs can include, but are not limited to fees for credit card transactions, hosting services or equipment costs, website and database application development and maintenance, customer support, implementing and maintaining merchant equipment, and Accounting Department time to process payments.

All development, maintenance, and support of web applications shall be the responsibility of the IT Department.

E-commerce related data that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure or modification in such a manner to prevent contract dispute and compromise of data.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO05.03, APO10.05, APO12.02, BAI02.05, BAI04.05, MEA03.01
GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2)

ISO 27001 6.1.2-3, 9.1-2, A.5.1.1, A.8.1, A.8.2.1, A.9, A.10.1, A.12.4

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 AC-1, AC-8, AU-1, CM-1, PA-1, RA-1, SA-1, SC-1, SI-1

NIST Cybersecurity Framework ID.AM-2, ID.AM-6, ID.GV-2, ID.RA-6, PR.AC-7, DE.DP-2

PCI 1.1, 1.3, 1.5, 2.1-3, 2.6, 3.1-2, 3.5, 3.7, 5.1-4, 6.1

E-MAIL POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Electronic mail (E-mail) is used as a means of communicating official company information to Staff, is convenient, rapid, environmentally aware, and cost effective. F2OnSite issues an e-mail address and disk space (for e-mail storage) to all Staff. F2OnSite also distributes e-mail software on computer systems. This practice ensures that all Staff have e-mail communication readily available to them. The purpose of this policy is to set forth the rights and responsibilities of both users and providers of electronic mail for Staff.

II. Purpose

This policy protects F2OnSite's e-mail related assets and helps ensure our ability to continue business operations including communications with Staff, suppliers, customers, the media, and other business contacts.

III. Scope

This policy applies to all Staff that have access to F2OnSite e-mail.

IV. Policy

A. COMPANY USES OF E-MAIL

F2OnSite uses electronic mail to communicate official F2OnSite information of many kinds to Staff and clients. Staff are responsible for reading their e mail on a frequent and regular basis, since some official communications may be time sensitive. F2OnSite suggests that Staff access their e-mail account on a daily basis.

B. FORWARDING OF E-MAIL MESSAGES

F2OnSite issues e-mail accounts and disk storage to all Staff. Staff must not forward e-mail from their F2OnSite e-mail address to a different e-mail address, such as one obtained from an external Internet Service Provider (e.g. AOL, gmail, Hotmail).

F2OnSite has no control over the delivery of e-mail that has been forwarded outside of our domain to external providers.

C. SECURITY AND PRIVACY

F2OnSite makes every effort to secure its computer systems, networked resources, and e-mail accounts, but cannot guarantee the infallibility of these systems to unauthorized intrusion, nor the authenticity of the sender of an electronic communication. For this reason e-mail is not appropriate for transmitting confidential or sensitive information of any kind. For example, e-mail should not be used to notify Staff of disciplinary or any other legal action.

Staff are responsible for keeping their e-mail passwords confidential, and should never share this information or access to Company resources with others, including friends and family members.

Without prior notice, F2OnSite reserves the right, but not the obligation, to routinely monitor and inspect individual accounts, files, and communications. Staff shall have no expectation of privacy in anything they store, send or receive on F2OnSite's e-mail system. F2OnSite may monitor messages without prior notice and is not obliged to monitor e-mail messages.

Spam filters shall be implemented to limit unwanted e-mail as well as reduce the likelihood Staff will perform actions such as clicking on e-mail html links or downloading malware attachments to their local devices.

D. E-MAIL RETENTION

This policy is intended to help Staff determine what information sent or received by e-mail should be retained and the appropriate retention period. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies. E-mail is categorized and retained according to the following guidelines.

Administrative correspondence - 3 years. Administrative correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All e-mail with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox adminemail@abccompany.com has been created, if you copy (cc) this address when you send e-mail, retention will be administered by the IT Department.

Financial correspondence - 7 years. Financial correspondence includes all information related to revenue and expense for F2OnSite. To ensure financial correspondence is

retained, a mailbox financeemail@ has been created, if you copy (cc) this address when you send e-mail, retention will be administered by the IT Department.

General correspondence - 1 year. General correspondence addresses information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for e-mail retention of general correspondence.

Refer to the Data Retention Policy for more information on archiving and retention requirements.

E. ENCRYPTED COMMUNICATIONS

In general, messages should be stored in a decrypted format. Encryption should be used to protect the transport of the message, not the storage. The security controls that protect the network will also protect the storage of the e-mail. Encrypted e-mail should be used when sensitive information is sent to non-company e-mail addresses.

International issues regarding encryption are complex. Staff shall follow corporate guidelines on export controls on cryptography, and consult the Legal Department for further guidance.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO05.03, APO10.05, APO12.02, BAI02.05, BAI04.05, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv)
ISO 27001 A13
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 AC-4, AC-20, AC-21, CA-3, PA-4, SC-7, SC-8
NIST Cybersecurity Framework ID.AM-2, ID.GV-4, PR.AC-1, PR.AC-4, PR.AC-7,
PR.DS-1-5
PCI 6.1, 6.2, 6.7

ENCRYPTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite information must be protected while stored and during transit. Encryption should be used to protect sensitive information.

II. Purpose

The purpose of this policy is to provide guidance on the use of encryption to protect F2OnSite's information resources that contain, process, or transmit confidential information. Additionally, this policy provides direction to ensure that regulations are followed.

III. Scope

This policy applies to all F2OnSite Staff. It addresses encryption policy and controls for confidential data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

IV. Policy

The Chief Security Officer shall ensure:

- Policies, procedures, and processes identify sensitive information that should be encrypted to protect against persons or programs that have not been granted access.
- The organization has implemented a mechanism to encrypt and decrypt sensitive information whenever deemed appropriate. Procedures specify how the organization transmits sensitive information as well as how often the information is transmitted.
- Based on the Risk Analysis, when encryption is needed to protect sensitive information during transmission. Procedures specify the methods of encryption used to protect the transmission of sensitive information.

- Logical access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column level database encryption.

A. KEY LENGTHS

F2OnSite uses software encryption technology to protect confidential and other sensitive data. To provide the highest level security while balancing throughput and response times, key lengths should be at least AES 256 bits for confidential data.

The use of proprietary encryption algorithms are not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the F2OnSite IT department.

B. DATA AT REST

Hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption avoids this problem.

Confidential data at rest on computer systems owned by and located within F2OnSite controlled spaces and networks should be protected by one or more of the following:

- Encryption
- Firewalls with strict access controls that authenticate the identity of those individuals accessing the data
- Sanitizing the data requiring protection during storage to prevent unauthorized exposure (e.g., truncating last four digits of a Primary Account Number).
- Other compensating controls including complex passwords, physical isolation/access, etc.

Using strong cryptography, all authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all Information Systems.

Password protection should be used in combination with all controls including encryption. Password protection alone is not an acceptable alternative to protecting confidential information.

F2OnSite secures its stored data on file systems, disks, and tape drives in servers and a Storage Area Network environment. All back up data is protected using AES 256-bit algorithm encryption methodologies.

Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure.

C. PORTABLE DEVICES

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential data are the result of stolen or lost Portable computing devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. As a general practice, confidential data should not be copied to or stored on a portable computing device or a non-F2OnSite owned computing device. However, in situations that require confidential data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

Each designated information resource owner shall identify information that is confidential. The information resource owner shall specify practices to include written authorization that verifies a legitimate business need for accessing and storing confidential information on a portable device and assesses the risk of unauthorized access to or loss of the data before granting permission for exceptions to this best practice.

All users must obtain specific permission from the data owner before storing confidential data on a portable computing device or a non-F2OnSite owned computing device.

Hard drives of portable devices (laptops and personal digital assistants (PDAs) must be encrypted using products and/or methods approved by F2OnSite's IT staff. Unless otherwise approved by IT management, such devices shall have full disk encryption with pre-boot authentication.

Portable devices should not be used for the long-term storage of any confidential information.

- Portable devices must have the proper protection mechanisms installed that include approved anti-malware software and firewall with unneeded services and ports turned off and properly configured applications.
- Removable media including CD's, DVD's, USB flash drives, etc. containing confidential information must be encrypted and stored in a secure, locked location. Such media must be transported in a secure manner.
- Portable or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).

F2OnSite shall inventory encrypted devices and validate implementation of encryption products at least annually.

Data owners and users of portable computing devices and non-F2OnSite owned computing devices containing confidential data must acknowledge how they ensure that data are encrypted and how encrypted data can be accessible by the owner in the event that an encryption key becomes lost or forgotten. Methods to meet this requirement include:

- Maintaining an accessible copy of the data.
- Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
- Escrowing the encryption key with a trusted party designated by the data owner and the F2OnSite IT management.

D. TRANSMISSION SECURITY

The Chief Security Officer (MGMT) shall ensure:

- Formal transfer policies, procedures, and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
- Users follow F2OnSite acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential data received from non-F2OnSite Staff.
- Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard sensitive data during transmission over open, public networks. Such controls include: Only trusted keys and certificates are accepted, the protocol in use only supports secure versions or configurations, and the encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include, but are not limited to, the Internet, Wireless technologies, including 802.11 and Bluetooth, cellular technologies (e.g. Global System for Mobile communications (GSM), Code division multiple access (CDMA)), General Packet Radio Service (GPRS), and satellite communications.
- Confidential information transmitted as an e-mail message is encrypted. Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with F2OnSite must be encrypted or be transmitted through an encrypted tunnel (VPN) or point-to-point tunnel protocols (PPTP) that include newer versions of transport layer security (TLS).
- Wireless (Wi-Fi) transmissions that are used to access F2OnSite portable computing devices or internal networks must be encrypted.
- Encryption is required when users access F2OnSite data remotely from a shared network, including connections from a Bluetooth device to a F2OnSite PDA or cell phone.

- The secure encrypted transfer of documents and data over the Internet using file transfer programs such as “secured FTP” (FTP over SSH) and secure copy command (SCP).
- All non-console administrative access such as browser/web based management tools are encrypted using strong cryptography.
- All implementations of SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.

E. ENCRYPTION KEY MANAGEMENT

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with the Electronic Data Retention Policy requirements. F2OnSite key management systems are characterized by following security precautions.

F2OnSite uses procedural controls to enforce the concepts of least privilege and separation of duties for personnel. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor personnel. IT security personnel shall verify backup storage for Key passwords, Files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.

Key management should be fully automated, e.g., IT personnel do not have the opportunity to expose a key or influence the key creation. Keys in storage and transit must be encrypted. Private keys must be kept confidential. Keys must be randomly chosen from the entire key space, using hardware-based randomization.

Key-encrypting keys are separate from data keys. No data ever appears in clear text that was encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure.

The resource Owner should be the person responsible for establishing data encryption policies that might include granting exceptions based upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data.

The Chief Security Officer (MGMT) shall ensure:

- Decryption keys are not associated with user accounts.
- Documentation and procedures exist to protect keys used to secure stored sensitive data against disclosure and misuse. This requirement applies to keys used to encrypt stored sensitive data, and also applies to key-encrypting keys used

to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.

- Restricted access to cryptographic keys to the fewest number of custodians necessary.
- Secret and private keys used to encrypt/decrypt sensitive data is stored in one (or more) of the following forms at all times: Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key, within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device), as at least two full-length key components or key shares, in accordance with an industry accepted method.
- Cryptographic keys are stored in the fewest possible locations.
- Key management processes and procedures for cryptographic keys are fully documented.
- Cryptographic key changes for keys that have reached the end of their crypto period (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
- Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.
- If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.
- The generation, use, and destruction of keys is based on proven processes.
- Cryptographic key custodians formally acknowledge that they understand and accept their key-custodian responsibilities.
- An annual evaluation of encryption algorithms and key sizes used within the organization.

F. ENCRYPTION OF DATA

Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. F2OnSite makes available software and procedures approved by the MGMT that provide robust encryption, as well as the capability for properly designated F2OnSite officials to decrypt the information when required and authorized under this policy. Users encrypting information shall only use the endorsed software and protocols. F2OnSite Staff may only encrypt with the permission of his or her supervisor. Data shall only be encrypted using F2OnSite approved software and procedures that provide the ability for F2OnSite to recover the data. Such endorsed software and procedures shall be updated as technical solutions and F2OnSite requirements change.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, APO12.02, APO13.07, APO14.01-02, APO14.07, MEA03.01
 GDPR Article 25, 32
 HIPAA 164.312(a)(2)(iv)
 ISO 27001 A.5.1.1, A.10
 NIST SP 800-37 3.4, 3.7
 NIST SP 800-53 SC-12, SC-13, SC-17
 NIST Cybersecurity Framework ID.GV-3, ID.RA-6, ID.RM-1, PR.DS-1-2, DE.DP-2
 PCI 2.1.1, 2.3, 3.4.1, 8.2.1, PCI Software Security Framework

ETHICS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to transparency, trust, and integrity. Our values and practices are the principles that guide our organization.

II. Purpose

This policy provides guidelines for Staff to help them conduct their actions in accordance with F2OnSite's primary values and ethical standards.

III. Scope

This policy applies to all F2OnSite Staff.

IV. Policy

F2OnSite's Executive Management shall be responsible for overseeing the development and implementation of a Code of Ethics. The Code of Ethics shall describe appropriate behavior principles when conducting organization business.

Accountability. Staff shall acknowledge and accept personal accountability for the ethical quality of their decisions and actions. Staff shall operate in the best interests of the organization and shall not take advantage of their position to personally benefit from organization activities.

Compliance. Staff shall use sound judgment, common sense, and comply with all relevant laws, regulations, and F2OnSite policies when conducting business.

Conduct. Staff shall operate in an honest, ethical, and fair approach when dealing and communicating with others. Staff shall not deliberately make untrue, misleading, deceptive, or fraudulent statements. In addition, Staff shall not manipulate, conceal, abuse, or misrepresent information or material facts. Staff shall protect the image and

reputation of the organization by ensuring conduct that builds respect and by taking actions necessary to correct or prevent inappropriate conduct of others.

Confidentiality. Staff shall be made aware of confidentiality requirements and take actions to ensure F2OnSite complies with such requirements. Information shall only be disclosed to authorized Staff on a need to know basis. Unauthorized disclosure of confidential information is prohibited. In the event of a breach of confidentiality, Staff shall immediately inform their immediate supervisor of any actions that create, or could create a breach of confidentiality.

Conflicts. Staff shall operate in the best interests of the Company and shall not engage in activities or actions that create a conflict of interest. Staff shall immediately inform their immediate supervisor of any actions that create, or could create, a conflict of interest.

Culture. F2OnSite values ethical behavior. Ethical values and behaviors shall be consistently and systemically supported by F2OnSite Executive Management. Staff shall respect the privacy, rights, and interests of others. Staff shall be courteous and treat others with respect and dignity regardless of sex, race, or national origin.

Records. Staff shall ensure that transactions and actions are accurately captured and reported for all relevant business activities. Such records shall be retained per F2OnSite's Data Retention Policy.

Violations. Any Staff member who becomes aware of a violation, or suspected violation, of this policy, or applicable laws or regulations, should immediately report the matter to their immediate supervisor.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01-03, APO01.01-02, APO01.05, APO01.09, MEA01.02, MEA03.01
 GDPR Article 23
 HIPAA 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(8), 164.316(a)
 ISO 27001 4.1, 5.1-2, 6.1.1, 6.1.3, 9.3
 NIST SP 800-37 2.1, 3.3, 3.5
 NIST SP 800-53 2.1, 3.2, 3.3, 3.9, 3.17
 NIST Cybersecurity Framework ID.AM-5, ID.BE-3, ID.GV-1, ID.GV-3
 PCI 3.1, 12.10

EU PRIVACY AND DATA PROTECTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, the European Commission, and Swiss Administration to provide organizations with a process to comply with privacy and data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

II. Purpose

Effective safeguards ensure that European Union (EU) subjects are protected from privacy and data breaches. The safeguards apply to all organizations processing the personal data of subjects residing in the EU regardless of the organization's location.

III. Scope

This policy applies to all F2OnSite Staff responsible for the security of F2OnSite's Information Resources.

IV. Policy

A. PRIVACY PRINCIPLES

Organizations that meet Privacy Shield requirements are deemed to provide "adequate" privacy protection, a requirement for the transfer of personal data outside of the European Union (EU) under the EU Data Protection Directive and outside of Switzerland under the Swiss Federal Act on Data Protection. EU Member State requirements for prior approval of data transfers either are waived or approval will be automatically granted.

The Privacy Shield program is administered by the U.S. International Trade Administration (ITA). The Privacy Shield Principles (Principles) include notice, choice,

accountability for onward transfer, security, data integrity and purpose, access, and recourse, enforcement and liability.

Notice. F2OnSite shall inform individuals about its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List. Such notice shall identify:

- The types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles.
- F2OnSite's commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.
- The purposes for which F2OnSite collects and uses personal information.
- How to contact F2OnSite with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.
- The type or identity of third parties F2OnSite discloses personal information, and the purpose.
- The right of individuals to access their personal data,
- Choices and means F2OnSite offers individuals for limiting the use and disclosure of their personal data.
- The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.
- The possibility, under certain conditions, for the individual to invoke binding arbitration,
- F2OnSite's requirement to disclose personal information in response to lawful requests by public authorities, including national security or law enforcement requirements.
- F2OnSite's liability in cases of onward transfers to third parties.

Choice. F2OnSite shall offer individuals a clear, conspicuous, and readily available mechanism to exercise the opportunity to opt out whenever their personal information is to be disclosed to a third party, or used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), F2OnSite must obtain affirmative opt-in express consent if such information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected or subsequently authorized by an individual through the exercise of opt-in choice. In addition, F2OnSite should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

Accountability for Onward Transfer. When transferring personal information to a third party acting as a controller (determines the purpose and means of the processing of personal data), F2OnSite must comply with the above Notice and Choice Principles. F2OnSite must also enter into a contract with the third party controller that provides such data shall only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles. The controller shall notify F2OnSite if it can no longer meet this obligation. Staff must:

- Transfer such data only for limited and specified purposes.
- Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles.
- Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the F2OnSite's obligations under the Principles.
- Require the agent to notify F2OnSite if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles.
- Take reasonable and appropriate steps to stop and remediate unauthorized processing.

Security. Staff must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

Data Integrity and Purpose. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. Staff shall not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by an individual. To the extent necessary for those purposes, Staff must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Staff must adhere to the Principles for as long as it retains such information per the Data Retention Policy.

Access. Individuals must have access and be able to correct, amend, or delete their personal information held by F2OnSite except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Recourse, Enforcement, and Liability. Effective privacy protection shall include robust mechanisms for assuring compliance with the Principles and recourse for individuals who are affected by non-compliance with the Principles. At a minimum such mechanisms must include:

- Readily available independent recourse mechanisms by which an individual's complaint/dispute is investigated and expeditiously resolved at no cost to the individual.
- Follow-up procedures for verifying F2OnSite privacy practice attestations and assertions are true and have been implemented as presented.
- Obligations to remedy problems arising out of failure to comply with the Principles.

Supplemental privacy considerations include sensitive data, journalistic exceptions, secondary liability, performing due diligence and conducting audits, the role of the Data Protection Authorities (DPA), self-certification, verification, access, Human Resources data, obligatory contracts for onward transfers, dispute resolution and enforcement, choice – timing of opt out, travel information, pharmaceutical and medical products, public record and publicly available information, and access requests by public authorities.

B. DATA PROTECTION

The Chief Security Officer (MGMT) and Chief Risk Officer (CRO) shall ensure that F2OnSite's privacy and data protection risks are properly managed and mitigated to the extent possible. The MGMT and CRO shall oversee the implementation and maintenance of formal policies including, but not limited to:

- Data classification – Data Classification Policy
- Access controls – Access Control Policy, Password Policy
- Business continuity – Business Continuity Policy
- Compliance – Compliance Policy
- Data retention – Data Retention Policy
- Disposal of sensitive information – Disposal Policy
- Incident management – Incident Response Policy
- Logging and monitoring – Logging Policy, Security Monitoring Policy
- Physical security – Physical Access Policy, Physical Security Policy
- Privacy – Data Privacy Policy, Privacy Policy
- Risk mitigation – Risk Assessment Policy, Risk Management Policy
- Security controls – Anti-Malware Policy, Backup Policy, Change Management Policy, Encryption Policy, Firewall Policy, Patch Management Policy, Ransomware Policy, Security Policy
- Security training – Security Awareness and Training Policy
- Service providers – Cloud Service Provider Policy, Third Party Service Providers Policy, Vendor Access Policy

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information and physical security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, MEA03.01
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D),
ISO 27001 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, DE.DP-2, RS.RP-1
PCI PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

FACILITY SECURITY PLAN

I. Introduction

F2Onsite is primarily a ‘Virtual’ company that does not operate within a specific physical location. these policies refer to our office location in Plano Texas, and shall apply when any employee is within the physical office.

A. Overview

This Facility Security Plan (Plan) describes the methods, procedures, and measures used to establish security measures and prevent loss, damage or compromise of assets and interruption to business activities.

This Plan is established to help ensure the organization can prevent loss of services and protect the integrity, availability and confidentiality of information. This Plan provides a well-defined and organized approach for implementing and maintaining controls that reduce threats to facilities and physical environment.

B. Risk Assessment

A risk assessment and risk analysis was performed to assess security risks, likelihood of events, and impact on our organization. The risk assessment identified risks to equipment, facilities, data, communications, servers, and many other types of Information Resources. The risk analysis identified preventive, detective, and corrective controls that treat risks.

C. Equipment

Equipment should e physically protected from security threats and environmental hazards. Protection of equipment, including that used off-site, is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. Special controls are required to protect against hazards or unauthorized access, and to safeguard supporting facilities.

D. Plan Updates

This Plan should be reviewed and updated on an annual basis. This Plan is reviewed, maintained, and updated by the VP of Corporate Security and Safety.

II. Facility Overview

A. Facility Information

F2OnSite is located at the address on the cover page of this Plan. The building is a mixed-use, multi-tenant facility. Current floor plans are on file with the Facilities Department.

B. Business Operations

Number of employees, contractors, and daily visitors on-site at this facility: [list quantity]

General functions performed at this facility: Administrative

C. Documentation

Policies and procedures should specify all physical security components that require documentation. Procedures should specify documentation of repairs and modifications to the physical components of a facility that are related to security (e.g. hardware, walls, doors, locks, cameras, alarms, etc.).

Procedures and related documentation should identify when special circumstances dictate repairs or modifications to physical security components are required. For example, when Staff with special privileges are terminated.

III. Personnel Considerations

A. Overview

F2OnSite is located at the address on the cover page of this Plan. The building is a mixed-use, multi-tenant facility. Current floor plans are on file with the Facilities Department.

B. Personnel Controls

A risk assessment and risk analysis should evaluate personnel related risks. The risk analysis and risk assessment should identify personnel related controls.

Documented procedures should control and validate a person's access to facilities is based on his/her role or function, including visitor control, and control of access to software programs for testing and revision. Procedures should control and validate a Staff member's access to facilities and consider guards, ID badges, key cards, etc. Procedures should specify visitor controls such as visitor sign in, wearing of visitor badges, escorting by authorized personnel, etc. On a periodic basis, management should review of the list of individuals with physical access to sensitive facilities.

Vehicles:

- **Public** – public parking is available in an unsecured parking lot. Lighting is available during evening hours.
- **Employees** – employees may park in a restricted parking lot available only to employees. The employee parking lot is restricted by means of attendant and gate. Numbers, not names or departments, are used to identify restricted spaces.

Entrances:

- **Entrances** – where possible, minimize the number of public entrances.
- **Screening** – consider the use of metal detectors and X-ray machines at public entrances.
As appropriate, security screening may also be performed at employee entrances.

Registration

- **Visitors** – visitors and other Staff (e.g. consultants, temporaries) without organization identification badges must sign in at the registration desk and show proof of identification.
- **Employees** – employees with identification badges may by-pass the registration desk.

Restricted access

- **Visitors** – visitors and other Staff must be escorted by organization personnel while on organization premises.
- **Employees** – employee identification badges are used as access cards. Each access card has been pre-programmed with appropriate rights that permit access to selected locations within the facility.

Shipping and receiving

- **Segregated** – shipping and receiving areas should be segregated from the main facility.
- **Access** – personnel in this area should not have direct access to other organization facilities.

C. Security Controls

As appropriate, management should implement security protection controls such as locked doors, signs warning of restricted areas, surveillance cameras, alarms, ID badges, visitor badges, escorts, and security services/patrols of the facility. Property controls such as property asset tags and engravings may also be implemented.

D. Mailing Handling

The Risk Assessment and Risk Analysis should evaluate other types of risks to facilities and Staff. The risk analysis should consider controls that reduce risks related to the items listed below.

Staff should be trained on how to identify suspicious mail. Examples include: mail with inappropriate or unusual labeling (e.g. excessive postage, misspelled words, no return address, titles with no name), or restrictive markings (e.g. “personal,” “confidential,” “do not x-ray”).

Staff should identify an unusual or inappropriate appearance (e.g. powdery substances felt through/on package, stains/discolorations, odors, excessive packaging material such as tape or string, bulky shape, ticking sounds, protruding wires, etc.).

Staff should be trained on how to handle suspicious packages and mail. Staff should not open, shake, show to others, or empty the contents of a suspicious letter or package. Instead, Staff should leave the letter or package where it is or gently place it on the nearest flat surface.

As appropriate, Staff should:

- Gently cover the letter or package using a waste basket or something similar.
- Shut off any fans or equipment in the area that may circulate the material.
- Alert others nearby to relocate to an area away from the suspicious item.
- Take essential belongings (e.g. cell phones, keys, and wallet) in case their return to the office is delayed.
- Immediately contact the Facilities Department.
- Leave the area and close the door to the space containing the suspicious letter or package.

E. Drills

Drills and exercises simulate realistic and fluid situations where critical decision-making is learned and Staff is familiarized with emergency response procedures. Exercises help to broaden a deeper understanding of response procedures and identify areas for improvement.

Drills can range from discussion based (e.g. table-top, workshop) to full-scale exercises that involve all Staff. Staff should periodically participate in drills and tests of procedures.

Examples include:

- Incident notification and activate appropriate alarms.
- Alarm response and building evacuation using exit routes posted throughout the facility.
- Business continuity testing of department and disaster recovery plans.

IV. Equipment Considerations

A. Overview

Equipment should be located or protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.

B. Equipment Controls

Preventive, detective, and corrective controls should be considered and implemented to protect equipment and facilities:

- Threats – controls should be implemented to minimize the risk of environmental and physical threats that include unauthorized access, theft, damage, fire, water, smoke, dust, vibration, chemicals, electrical interference, electromagnetic radiation, and similar risks.
- Location – equipment should be located to minimize unnecessary access by authorized and unauthorized staff. The impact of terrorism, collateral damage, and similar threats should be evaluated when considering equipment location.
- Special needs – equipment that requires special security protection should be identified and isolated to reduce the likelihood of compromise.
- Personnel – Staff that implement, manage, and maintain equipment and facilities shall be properly trained.
- Prohibited activities – activities such as smoking, eating and drinking should be banned in or near Information Systems.
- Monitoring – environmental systems should be identified and monitored to ensure proper and continued delivery of services. Failover or redundant systems should be considered where there is a greater chance of downtime or impact on the organization.

C. Disaster Controls

In the event of a disaster, the Business Continuity Disaster Recovery Plan identifies Emergency Action Facility Team procedures that address the salvage or replacement of equipment, network server room facilities, etc. Such procedures include:

- Working with Company management to identify options (repair existing or identify replacement) facilities.
- Working with outside vendors as appropriate for environmental, power and repair conditions.

V. Environmental Considerations

A. Overview

Information Systems and data centers have special environmental considerations. Equipment should be protected from power failures, air conditioning outages, fires, and similar types of threats.

B. Power Controls

A reliable power source should be provided that conforms to equipment manufacturer requirements. Redundant and fail over systems can include:

- Power – power feeds from several suppliers.
- Generators – backup power generators.
- Uninterruptible Power – Uninterruptible Power Supply (UPS) on servers, critical networking equipment, and important workstations.

Power feeds. Power sources are generally classified into the following categories:

- Single feed from a single substation. This option presents the greatest risk as the power supply has numerous single points of failure.
- Single substation with two feeds. By having two separate feeds, the data center reduces the risk of a single line failure. However, this configuration only uses one substation as the power source.
- Dual substations. Two substations provide an additional level of redundancy over a single substation. This reduces the likelihood of a prolonged outage due to the failure of a single substation or its respective feed.
- Dual Feed. Power is supplied by two separate substations with a single independent feed from each. Power from both substations is fed directly into each of transformers located inside the building. There are no single points of failure and power loads within the facility are shared.

Generator. A backup generator can be used to provide power during prolonged power outages. If installed, generators should be installed by licensed professionals and regularly tested in accordance with the manufacturer's instructions. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period of time.

Uninterruptible Power Supply (UPS). A UPS uses batteries to provide power to critical systems for a limited amount of time. UPS systems can allow an orderly and controlled shut down of systems either manually or automatically. UPS systems should be tested on a regular basis to ensure they offer adequate capacity. Batteries should be replaced as needed.

Other power related considerations include:

- Equipment room emergency power switches should be located near emergency exits. In the event of an emergency, Staff can hit the switch to rapidly shut down power.

- Emergency lighting should be automatically activated in the event of a power failure.
- Lightning protection should be installed at all facilities. Lightning protection filters should be installed on all external communication lines.

C. Heating and Air Conditioning System Controls

The required heating and/or cooling load is largely determined by the amount of floor space. In some instances, particularly in buildings with high ceilings, the volume of the space should be considered. In addition to measuring the area, consider heat transfer through walls, doors and roofs, lighting systems, IT equipment, and occupancy levels. Heating and air conditioning systems should be positioned so they are only accessible by authorized personnel and should be maintained per manufacturer requirements.

D. Water Controls

The organization should evaluate water related risks and controls including:

- Dependence on water quality, quantity, and cost.
- Redundant water supply sources including water trucks.
- Miscellaneous factors that may impact operations including water rights and legal obligations.

VI. Cabling Considerations

A. Overview

Power and telecommunications cabling carrying data or support information services should be protected from interception or damage.

B. Power and Telecommunications Controls

The following controls should be considered to protect against disruption in service or unauthorized interception of communications:

- Protection – where possible, cables to the facility should be underground.
- Network cabling – should be protected by conduit or other means. Where possible, routes should avoid public areas.
- Separation – power cables should be separated from communications cables to prevent interference.

C. Sensitive or Critical Systems

Sensitive or critical systems may require additional controls including:

- Protection – armored conduit, locked closets, and boxes at inspection and termination points. Fiber optic instead of less secure Ethernet cabling.
- Redundancy – use of alternative routings or transmission media or solutions (e.g. wireless).
- Detection – periodic physical and electronic detection of unauthorized devices.

VII. Maintenance Considerations

A. Overview

Equipment should be properly maintained to ensure its continued availability, integrity, improved productivity, and reduced environmental impact. All equipment shall be maintained in an efficient state and in good working order. Maintenance logs shall be maintained and kept up-to-date.

B. Frequency

The frequency and nature of maintenance activities should be determined through a risk assessment of the equipment that considers:

- Manufacturer recommendations.
- Requirements imposed by insurance policies.
- Intensity of use of the equipment.
- Operating environment (e.g. temperature, corrosion, weathering).
- User knowledge and experience.
- Risk to health/safety from any foreseeable failure or malfunction.

C. Maintenance Controls

The following equipment maintenance controls should be considered:

- Equipment should be maintained in accordance with the manufacturer's recommended service intervals and specifications.
- Only authorized maintenance personnel should carry out repairs and service equipment.
- Records should be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate controls should be taken when sending equipment off-site for maintenance.

VIII. Off-site Considerations

A. Overview

Management must pre-authorize the use of equipment that will be used or hosted off-site of F2OnSite's premises. Where possible, the security provided should be equivalent to that for equipment used or hosted on-site at our location.

When making the decision to allow equipment to be used or hosted off-site, management should consider the risks of Staff working off-site.

B. Off-site Controls

Where possible, the following controls should be implemented for off-site equipment:

- Equipment and media taken off the premises should not be left unattended in public places. Portable computers, tablets, media, etc. should be hand carried and not checked in luggage when traveling.
- Staff shall follow manufacturer instructions for protecting equipment (e.g. temperature, proximity to strong electromagnetic fields, etc.).
- Off-site controls (e.g. locking filing cabinets, Clear Desk Policy, access controls for Information Systems) should be applied.
- Adequate insurance should be in place to protect off-site equipment.

Security risks including damage, theft, eavesdropping, etc. may vary considerably between locations and should be taken into account when determining the most appropriate controls.

IX. Equipment Disposal/Re-use Considerations

A. Overview

Information can be compromised through careless disposal or re-use of equipment. Storage devices containing sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function.

B. Disposal/Re-use Controls

Equipment and media should be properly disposed of considering manufacturer and environmental requirements. The nature of disposal/re-use procedures should be determined through a risk assessment of the equipment/media that considers:

- Intended re-use of the device/media.
- Sensitive data stored on the device/media.
- Licensed software stored on the device/media.
- Compliance requirements.

Storage media (e.g. hard drives, flash drives, etc.) should be checked to ensure that any sensitive data and licensed software have been securely removed or overwritten prior to disposal or re-use.

Damaged storage devices containing sensitive data may require a risk assessment to determine if the items should be destroyed, repaired or discarded.

Appendix A – Supporting Documents

This Plan is part of an overall approach to managing business and operational risks. Organization policies, plans, and forms provide additional direction and guidance. Examples of documents that support this Plan include, but are not limited to:

- Acquisition and Procurement Policy
- Business Continuity Policy
- Disaster Recovery Plan
- Disposal Policy
- Documentation Policy
- Hardware and Software Maintenance Policy
- Incident Response Plan
- Incident Response Policy
- Personnel Security Policy
- Physical Access Policy
- Physical Security Policy

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Facility Security Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

Executed by any employees who work more than 50% on the F2OnSite Premises

FIREWALL HARDENING PROCEDURE

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Firewall policies provide management direction and guidance to ensure systems and data are properly protected. Procedures document a detailed description of the steps necessary to perform specific operations that comply with F2OnSite's firewall related policies.

II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in F2OnSite's Firewall Policy.

III. Scope

This procedure applies to all F2OnSite Staff who administer firewalls.

IV. Procedure

Physical security. Ensure the firewall is placed in a physical location that restricts access to authorized individuals. Where possible, consider a locking cabinet/rack in a secure data center.

Alerts, advisories, and vulnerability announcements. Monitor manufacturer alerts, advisories, and vulnerability announcements. Ensure patches and updates are installed in a timely manner.

Logging and monitoring. Ensure logging is activated per the Logging Policy. Consider centralized logging that consolidates logs for analysis and incident tracking. Log messages may be assigned a severity level whereby specific messages, based on their severity, are sent to remote logging servers. By default, these messages may be transmitted in clear text. Where possible, encryption should be used when transmitting messages. Unless required, firewall administrators should generally avoid logging messages at a debug level as this can produce a high load on the device.

Protocols and services. Document authorized inbound and outbound activity and only allow authorized ports/services to be open. All other inbound and outbound ports/services should be closed. Use secure protocols such as Secure Shell (SSH) and Secure File Transfer Protocol (SFTP).

Authentication. Ensure a long and complex memorized secret (i.e. password) is used to administer the device. Ensure default credentials are changed.

Lockout. If the device has a lockout feature, activate the lockout where the account is locked after a number of failed or invalid logon attempts.

Session timeout. Sessions should be terminated after a period of inactivity (e.g. 5 minutes).

Time. An accurate time and date is important for system and event logs. Configure a trusted time source for Network Time Protocol (NTP) and use proper authentication.

CPU notification. If available as a feature, activate the feature that allows an administrator to be notified if the CPU load exceeds a set threshold for a period of time.

Management sessions. Administrators should not connect to the device using unsecure services such as http or telnet as communications are not encrypted.

Accountability. Each firewall administrator should use their own unique administrator account when managing the firewall. This provides an audit trail with accountability.

Console ports. Console ports may provide special administrator privileges such as the recovery of passwords. The firewall administrator should ensure only secure local and remote access to the console port is permitted.

Warning banners/notices. Some implementations may require the use of warning banners or notices. Firewall administrators should consult with F2OnSite legal staff regarding the posting of notices such as:

- Access is only permitted by authorized personnel
- Activities are logged and monitored and can be used as evidence
- Unauthorized access or use can result in civil and criminal penalties

Backup. A copy of the device configuration should be saved on a separate and secure location to assist in a recovery effort if needed.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening firewalls and specific security functionality.

V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

VI. Distribution

This procedure is to be distributed to all F2OnSite Staff who administer firewalls.

Procedure History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial procedure release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.312(d), 164.312(e)(2)(i)
ISO 27001 6.1.3, A.9.1.2
NIST 800-41 4, 5
NIST SP 800-53 AC-3, AC-4, AC-5, CA-3, CM-7, SA-9, SC-7, SC-28
NIST Cybersecurity Framework ID.RA-1, PR.AC-3, PR.AC-5, PR.DS-1-2, DE.DP-2, RS.RP-1
PCI 1.1-3, 2.1

FIREWALL POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Firewalls are hardware devices or software programs that control the flow of traffic between networks, servers, and computer systems.

II. Purpose

This policy helps protect F2OnSite's Information Resources and related information asset availability, confidentiality, and integrity.

III. Scope

This policy applies to all Staff responsible for security and protecting F2OnSite's Information Resources.

IV. Policy

F2OnSite uses a multi-layered approach to protect Information Resources and related "information assets". At one time, most firewalls were deployed at network perimeters. This provided some measure of protection for internal hosts, but did not recognize all instances and forms of attack when attacks were sent from one internal host to another and did not pass through network firewalls. Network security design shall include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect devices that are placed directly onto external networks.

The Chief Security Officer (MGMT) shall ensure the following controls are in place:

- A formal process for approving and testing all network connections and changes to the firewall and configurations.
- A current network diagram identifies all connections between environments containing sensitive data and other networks, including any wireless networks.

- A diagram documents sensitive data flows across systems and networks.
- Firewalls are positioned at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
- Description of groups, roles, and responsibilities for management of network components.
- Documentation and business justification for use of all services, protocols, and ports/services allowed, including documentation for security features implemented for those protocols considered to be insecure.
- Examples of insecure services, protocols, or ports that include, but are not limited to, FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
- Procedures review firewall configurations at least every six months.
- A standard configuration exists for fast and consistent firewall deployment.
- Critical firewalls have been identified and are under maintenance/replacement contracts.
- Subscriptions/licenses satisfy business requirements.

IT security Staff shall define how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. IT security Staff shall:

- Restrict inbound and outbound traffic to that which is necessary for sensitive data and specifically deny all other traffic.
- Install perimeter firewalls between any all wireless networks and sensitive data and configure these firewalls to deny or, control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment and environments containing sensitive data.

The IT Director shall conduct a risk analysis to develop a list of the types of traffic needed by the organization and how they must be secured. The risk analysis shall include which types of traffic can traverse a firewall under what circumstances. Generally, all inbound and outbound traffic not expressly required should be blocked. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the organization's networks.

IT security Staff shall identify the requirements that should be considered when determining the types of firewall to be implemented. IT security Staff should consider network related assets as well as the firewall technologies most effective at blocking network related threats. IT security Staff shall consider performance considerations as well as concerns regarding the integration of the firewall into existing network and security infrastructures. The firewall solution design should involve requirements related

to F2OnSite's physical environment and personnel as well as consideration of possible future needs, virtual private networks (VPN), etc.

IT security Staff shall create network traffic rules that are as specific as possible. IT security Staff shall consider the types of traffic required and protocols the firewall may need to use for management purposes.

IT security Staff is responsible for managing the firewall architectures, policies, software, and other components throughout the life of the firewall solutions. There are many aspects to firewall management. For example, choosing the type or types of firewalls to deploy and their positions within the network can significantly affect the security policies that the firewalls can enforce. Policy rules may need to be updated as F2OnSite's requirements change, when new applications or servers are implemented within the network, etc.

Firewall performance should be monitored to ensure availability of F2OnSite's Information Resources. If possible, monitoring tools shall be used to monitor issues and take action before components become overwhelmed. Logs and alerts should also be continuously monitored to identify threats, both successful and unsuccessful.

Firewall rules and policies should be managed by a formal change management control process because of their potential to impact security and business operations, with rules, reviews, or tests performed periodically to ensure continued compliance with the organization's policies. Firewall software should be patched as vendors provide updates to address vulnerabilities.

Configurations shall prohibit direct public access between public networks (e.g. Internet) and any Information Resource containing sensitive information. A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to limit network access to devices that store sensitive data.

Configurations shall restrict all traffic, inbound and outbound, from untrusted networks (including wireless) and hosts and specifically deny all other traffic except for necessary protocols.

IT security Staff shall:

- Implement a demilitarized zone (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports/services.
- Limit inbound Internet traffic to IP addresses within the DMZ.
- Not allow any direct connections, inbound or outbound, for traffic between the Internet and the environments containing sensitive data.
- Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

- Not allow unauthorized outbound traffic from environments containing sensitive data to the Internet.
- Use stateful inspection, also known as dynamic packet filtering, so that only "established" connections are allowed into the network.
- Ensure system components that store sensitive data (e.g. database) in an internal network zone, segregated from the DMZ and other untrusted networks.
- Configure systems to not disclose private IP addresses and routing information to unauthorized parties. Methods to obscure IP addressing may include, but are not limited to Network Address Translation (NAT), placing servers containing sensitive data behind proxy servers/firewalls, removal or filtering of route advertisements for private networks that employ registered addressing, and internal use of RFC1918 address space instead of registered addresses.

Physical access to hardware firewall devices must be restricted as much as possible. Desktops, laptops, and similar devices should have software firewalls installed. These software firewalls provide an additional layer of protection and must not be disabled without prior authorization from IT security Staff.

Firewall security log files must be configured, maintained, and periodically reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event.

IT security Staff shall receive periodic training regarding new and developing threats, current data security practices, and changes in compliance regulations.

IT security Staff shall ensure:

- Formal firewall hardening procedures are in place.
- Formal testing procedures are followed whenever configurations change.
- Firewall passwords are long and complex. Default passwords and configurations are changed on all firewalls.
- Firewalls are patched and updated in a timely manner. Documentation and procedures ensure that software updates and maintenance procedures are performed by authorized personnel.
- Firewalls under support contract with appropriate response time guarantees.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite security Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.312(d), 164.312(e)(2)(i)
ISO 27001 6.1.3, A.9.1.2
NIST 800-41 4, 5
NIST SP 800-53 AC-3, AC-4, AC-5, CA-3, CM-7, SA-9, SC-7, SC-28
NIST Cybersecurity Framework ID.RA-1, PR.AC-3, PR.AC-5, PR.DS-1-2, DE.DP-2, RS.RP-1
PCI 1.1-3, 2.1

FORMS

- Asset Transfer Form
- Audit Log Form
- Backup Log Form
- Business Impact Analysis Questionnaire
- Change Management Log Form
- Incident Response Form
- Information Systems Access Request Form
- Information Systems Log Form
- Problem Management Form
- Third Party Service Provider Log Form

Asset Transfer Form

I. Purpose

This form is used to maintain a record of F2OnSite asset transfers.

II. Description of Transfer

A. TYPE OF TRANSFER

Select type of request

- ☐ Information System (e.g. servers, routers, switches, hubs, applications, etc.)
- ☐ Environmental (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms)
- ☐ Other (describe) _____

B. NATURE OF TRANSFER

Date Requested: _____

Nature of Transfer: _____

Resource Owner: _____

Date approved by Change Management Committee: _____

III. Action Taken

Date and Time	Action(s) Taken (include from and to locations)	Completed By	Status (Success/Fail)

Audit Log Form

I. Purpose

This log is used to maintain a record of security audits, vulnerability assessments, and penetration tests.

II. Evaluation History

Date(s) of evaluation	Type of evaluation performed (security audit, vulnerability assessment, penetration test, etc.)	Important issues identified	Assigned Staff	Estimated completion date(s)

Business Impact Analysis Questionnaire Form

I. Purpose

This form is used to help identify the business processes and applications that are essential to the survival of the business, the amount of acceptable data loss (recovery point objective), and the speed at which systems must be restored (recovery time objective).

Business impacts are identified based on a worst-case scenario assuming that the infrastructure supporting each department has been destroyed and all records, equipment, etc. are not immediately accessible.

II. Department Information

Background

Department _____

Representative(s) _____

Major department processes

Procedures

Does the department have documented manual procedures that could be used as “workarounds” in the event IT services are interrupted? Are the procedures stored off-site? When were the procedures last tested?

If no If no manual procedures exist for your business function, estimate the number of workdays it would take to develop them. Also indicate any other important factors.

Critical Personnel

What are the minimum number of employees required (critical personnel) to keep the department operational to the point that the impact on the organization is minimal during a prolonged outage? In a disaster, each employee is assumed to require a desk, computer, phone, and access to a printer, the Internet, and e-mail. Are there other unique resources required at the time of a disaster?

III. Resources Needed

Resource	Acceptable downtime of Resource before issue becomes high priority	Acceptable data loss before issue becomes high priority	Financial impact or other implication
Facilities (work area)		NA	
Phones		NA	
Internet connectivity		NA	
Special equipment or peripherals			
Application 1			
Application 2			
Application 3			
Service Provider 1			
Service Provider 2			
Other			

Change Management Log Form

I. Purpose

This log is used to maintain a record of changes to Information Resources (e.g. operating system, computing hardware, networks, applications, data centers).

II. Description of Change

A. TYPE OF CHANGE

Select type of request

- ☐ Information System (e.g. servers, routers, switches, hubs, applications, etc.)
- ☐ Environmental (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms)
- ☐ Other (describe) _____

B. NATURE OF CHANGE

Date Requested: _____

Nature of change: _____

Resource Owner: _____

Date approved by Change Management Committee: _____

III. Action Taken

Date and Time	Action(s) Taken	Completed By	Status (Success/Fail)

Incident Response Form

I. Purpose

This form is used to identify incidents, classify, and document actions taken.

II. Description of Incident

A. TYPE OF INCIDENT

Select type of incident

- ☐ Network Infrastructure (e.g. firewalls, IDS/IPS, routers, switches, hubs)
- ☐ Server (e.g., file server, database server, application server, etc.)
- ☐ Application (e.g. internal software, cloud service, Web site, etc.)
- ☐ Security Protection (e.g. anti-malware, backups, cameras, etc.)
- ☐ Other (describe)

B. NATURE OF INCIDENT

Date Identified:

Individual(s) reporting incident:

Description of incident:

Resource Owner:

III. Action Taken

Document actions taken including:

- Incident: notification, classification, declaration (a formal Incident is declared)
- Incident response: alert, triage, response, recovery, maintenance
- Considerations: systems impacted and the extent of damage or breach, how the breach occurred, steps taken to mitigate or remedy the situation, suspects (internal or external), evidence that exists or needs to be preserved.

Date and Time	Action(s) Taken	Performed By

Information Systems Access Request Form

I. Purpose

This form should be used when requesting authorization for additional access to F2OnSite Information Systems, making changes to existing access, removing access, or for a user name change.

II. Request Type

Select type of request

- ☐ New access
- ☐ Change existing access
- ☐ Terminate access
- ☐ Other (describe) _____

III. Account Information

CONTACT

Individual's Name: _____

Individual's Department/Organization: _____

DESIRED ACCESS PRIVILEGES

- ☐ E-mail
- ☐ Internet access
- ☐ Wireless access
- ☐ Microsoft Office
- ☐ Software Application
- ☐ Software Application
- ☐ Software Application
- ☐

IV. Approval

Supervisor's Name: _____

Supervisor's Signature: _____ Date: _____

V. IT Department

Date Received	Action Taken	Date Completed	Completed By

Problem Management Form

I. Purpose

This form is used to identify problems, classify, determine impact, and document actions taken.

II. Description of Problem

A. TYPE OF PROBLEM

Select type of problem

- ☐ User related (e.g. can't log on, device not working, lost device, etc.)
- ☐ Network Infrastructure (e.g. firewalls, IDS/IPS, routers, switches, hubs)
- ☐ Server (e.g., file server, database server, application server, etc.)
- ☐ Application (e.g. internal software, cloud service, Web site, etc.)
- ☐ Security Protection (e.g. anti-malware, backups, cameras, etc.)
- ☐ Other (describe)

B. NATURE OF PROBLEM

ID (tracking or ticket number):

Date Identified:

Individual(s) reporting problem:

Description of problem:

Resource Owner:

III. Action Taken

Document actions taken including:

- Problem notification, classification
- Problem information: service/equipment details
- Considerations: staff and systems involved, impact on the organization, solution/steps taken to address the situation, documentation that exists or needs to be preserved

Date and Time	Action(s) Taken	Performed By

GDPR EU PRIVACY AND DATA PROTECTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, the European Commission, and Swiss Administration to provide organizations with a process to comply with privacy and data protection requirements when transferring personal data from the European Union and Switzerland to the United States.

II. Purpose

Effective safeguards ensure that European Union (EU) subjects are protected from privacy and data breaches. The safeguards apply to all organizations processing the personal data of subjects residing in the EU regardless of the organization's location.

III. Scope

This policy applies to F2OnSite Executive Management, Department Heads, the Chief Security Officer, Risk Management Officer, Data Protection Officer, and those responsible for information and physical security.

IV. Policy

A. PRIVACY PRINCIPLES

Organizations that meet Privacy Shield requirements are deemed to provide "adequate" privacy protection, a requirement for the transfer of personal data outside of the European Union (EU) under the EU Data Protection Directive and outside of Switzerland under the Swiss Federal Act on Data Protection. EU Member State requirements for prior approval of data transfers either are waived or approval will be automatically granted.

The Privacy Shield program is administered by the U.S. International Trade Administration (ITA). The Privacy Shield Principles (Principles) include notice, choice,

accountability for onward transfer, security, data integrity and purpose, access, and recourse, enforcement and liability.

Notice. F2OnSite shall inform individuals about its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List. Such notice shall identify:

- The types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles.
- F2OnSite's commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.
- The purposes for which F2OnSite collects and uses personal information.
- How to contact F2OnSite with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.
- The type or identity of third parties F2OnSite discloses personal information, and the purpose.
- The right of individuals to access their personal data,
- Choices and means F2OnSite offers individuals for limiting the use and disclosure of their personal data.
- The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.
- The possibility, under certain conditions, for the individual to invoke binding arbitration,
- F2OnSite's requirement to disclose personal information in response to lawful requests by public authorities, including national security or law enforcement requirements.
- F2OnSite's liability in cases of onward transfers to third parties.

Choice. F2OnSite shall offer individuals a clear, conspicuous, and readily available mechanism to exercise the opportunity to opt out whenever their personal information is to be disclosed to a third party, or used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), F2OnSite must obtain affirmative opt-in express consent if such information is to be disclosed to a third party or used for a purpose other than that for which it was originally collected or subsequently authorized by an individual through the exercise of opt-in choice. In addition, F2OnSite should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

Accountability for Onward Transfer. When transferring personal information to a third party acting as a controller (determines the purpose and means of the processing of personal data), F2OnSite must comply with the above Notice and Choice Principles. F2OnSite must also enter into a contract with the third party controller that provides such data shall only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles. The controller shall notify F2OnSite if it can no longer meet this obligation. Staff must:

- Transfer such data only for limited and specified purposes.
- Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles.
- Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the F2OnSite's obligations under the Principles.
- Require the agent to notify F2OnSite if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles.
- Take reasonable and appropriate steps to stop and remediate unauthorized processing.

Security. Staff must take reasonable and appropriate measures to protect data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

Data Integrity and Purpose. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing. Staff shall not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by an individual. To the extent necessary for those purposes, Staff must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Staff must adhere to the Principles for as long as it retains such information per the Data Retention Policy.

Access. Individuals must have access and be able to correct, amend, or delete their personal information held by F2OnSite except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Recourse, Enforcement, and Liability. Effective privacy protection shall include robust mechanisms for assuring compliance with the Principles and recourse for individuals who are affected by non-compliance with the Principles. At a minimum such mechanisms must include:

- Readily available independent recourse mechanisms by which an individual's complaint/dispute is investigated and expeditiously resolved at no cost to the individual.
- Follow-up procedures for verifying F2OnSite privacy practice attestations and assertions are true and have been implemented as presented.
- Obligations to remedy problems arising out of failure to comply with the Principles.

Supplemental privacy considerations include sensitive data, journalistic exceptions, secondary liability, performing due diligence and conducting audits, the role of the Data Protection Authorities (DPA), self-certification, verification, access, Human Resources data, obligatory contracts for onward transfers, dispute resolution and enforcement, choice – timing of opt out, travel information, pharmaceutical and medical products, public record and publicly available information, and access requests by public authorities.

B. DATA PROTECTION OFFICER

Executive Management shall ensure a role based job description for a Data Protection Officer is implemented and maintained.

- The data protection officer shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices.
- The data protection officer may be a Staff member of the organization or fulfil the tasks on the basis of a service contract.
- The organization shall publish the contact details of the Data Protection Officer and communicate them to the supervisory authority.

C. DATA PROTECTION TECHNICAL AND ORGANIZATIONAL MEASURES

The Chief Security Officer (MGMT), Risk Management Officer (RMO), and Data Protection Officer (DPO) shall ensure that F2OnSite's privacy and data protection risks are properly managed and mitigated to the extent possible.

Security measures shall include but not be limited to:

- Documents (e.g. agreements, disclosure) that specify the specific purpose for collecting personal data and the minimum amount of personal data to be collected and processed.
- An analysis is performed to determine if special categories (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) of personal data are processed.
- Written procedures that ensure personal data remains accurate. Written procedures shall also ensure inaccurate data is corrected or deleted in a timely manner.
- Data flow diagrams document business processes that transmit, receive, create, modify, delete, and access personal data.
- Processes shall ensure that personal data remains secure throughout its lifecycle including data collection, processing, storage, transmission, and disposal.

- An analysis to determine when pseudonymization and encryption shall be used to protect personal data.
- Ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- Restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- Assessing the appropriate level of security, identifying risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored or otherwise processed.
- Ensuring that persons who have access to personal data do not process the data except on approved instructions.

The MGMT, RMO, and DPO shall oversee the implementation and maintenance of formal policies including, but not limited to:

- Data classification – Data Classification Policy
- Access controls – Access Control Policy, Password Policy
- Business continuity – Business Continuity Policy
- Compliance – Compliance Policy
- Data retention – Data Retention Policy
- Disposal of sensitive information – Disposal Policy
- Incident management – Incident Response Policy
- Logging and monitoring – Logging Policy, Security Monitoring Policy
- Physical security – Physical Access Policy, Physical Security Policy
- Privacy – Data Privacy Policy, Privacy Policy
- Risk mitigation – Risk Assessment Policy, Risk Management Policy
- Security controls – Anti-Malware Policy, Backup Policy, Change Management Policy, Encryption Policy, Firewall Policy, Patch Management Policy, Ransomware Policy, Security Policy
- Security training – Security Awareness and Training Policy
- Service providers – Cloud Service Provider Policy, Third Party Service Providers Policy, Vendor Access Policy

D. DATA PROTECTION IMPACT ASSESSMENT

Staff shall seek the advice of the Data Protection Officer when carrying out a Data Protection Impact Assessment. A Data Protection Impact Assessment shall be required in the case of:

- A systematic and extensive evaluation of personal aspects which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the person or similarly significantly affect the natural person, or

- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offenses, or
- A systematic monitoring of a publicly accessible area on a large scale.

The Data Protection Impact assessment shall contain at least:

- A systematic description of the envisioned processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the Controller.
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects.
- The measures envisioned to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulation (GDPR).

Where necessary, Staff shall carry out a review to assess if processing is performed in accordance with the Data Protection Impact Assessment at least when there is a change of the risk represented by processing operations.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite Executive Management, Department Heads, the Chief Security Officer, Risk Management Officer, Data Protection Officer, and those responsible for information and physical security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, MEA03.01
 GDPR Article 25, 30, 32
 HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D),
 ISO 27001 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18
 NIST SP 800-37 3.4, 3.7
 NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
 NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, DE.DP-2, RS.RP-1
 PCI PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

GREEN COMPUTING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to the social, environmental and economic well-being of the global community in which our Staff live and work.

II. Purpose

To help reduce F2OnSite's carbon footprint, save costs related to energy consumption, and extend the life of computers and other equipment, F2OnSite requires Staff to follow energy efficient computing strategies. We encourage employees to apply the same principles of energy conservation to shared-use devices within our office environments.

III. Scope

This policy applies to all Staff that use and manage F2OnSite's Information Resources.

IV. Policy

Computers and other office machinery consume power and generate heat whenever they are on. Employees should seek to optimize the power consumption of office machinery to reduce the waste, environmental impact, and energy costs associated with its use. Even small changes to the way Staff use and manage common devices can significantly reduce the amount of energy consumed by office machines.

A. DESKTOP (PERSONAL) COMPUTER USAGE AND MANAGEMENT

- The configuration of desktop and laptop machines shall be standardized so that power-saving and/or energy management settings support energy-efficient operation. Computers should be configured to enact “sleep” or “hibernation” mode whenever the computer is not in use for more than 15 minutes or the minimum amount of time that does not impede typical work performance.

- If screen savers are not in place, Staff shall turn off computer monitors when not in use during breaks, meetings, and other periods when they are away from their computer for 15 minutes or more.
- When purchasing new equipment, Department heads shall request peripherals that offer power saving or sleep modes. Devices shall be configured to active these modes at the minimal time that does not impede work performance.
- Prior to leaving for the day, Staff shall turn off workstations and other peripherals that do not run processes during the evening.
- Staff shall use e-mail or other electronic communication media whenever practical as an alternative to paper memos and faxes.

B. SHARED-USE OFFICE DEVICES

- Staff shall use the “print preview” function built into office applications to review documents before printing. This process ensures page formatting is correct prior to printing hard copy pages.
- Staff shall avoid printing e-mail messages and other electronic documents unless there is a specific need to retain the document or distribute a hard copy.
- If available, Staff shall use the duplex, two-sided printing feature.
- Copiers, faxes, and shared-use office devices should be turned on only when needed. On a daily basis, the first person who requires the use of such a device shall turn it on.
- Staff should turn off shared-use devices at the end of each work day.

C. IT DEPARTMENT

- The IT Department should factor energy efficiency and utility cost savings into technology decisions. IT Department staff shall evaluate, and implement where possible, virtualization technologies that allow server consolidation, improve operating efficiency, and reduce space requirements in data center environments.
- Software development managers shall consider the need for information availability. When possible, resources or processes that may be made periodically unavailable (e.g., overnight, on weekends, and over holidays) shall be hosted on servers that can be periodically shut down to reduce energy consumption.
- The IT Department shall review and document utilization statistics on data center equipment. Inefficient use of server resources shall be brought to the attention of the IT Director.
- Data that has not been accessed at least once in the past year shall be archived by the IT Department Staff to off-line storage.

- IT Department Staff shall evaluate servers that do not support 24×7 operations to determine if they may be turned off after work hours, over weekends, and during holidays without interfering with normal business functions.

IT Department Staff shall measure, track, document, and report electrical consumption by the data center. Such reports shall provide comparative metrics for:

- Energy consumption by the entire data center over time, and
- Electricity consumption by individual machines within the data center (if possible).

The above reports shall note and report any energy consumption by data center machines that might indicate the impending failure of a machine or the need to replace a machine with a more energy-efficient alternative. The report shall also provide recommendations for specific actions to reduce electricity consumption in the data center, either by computing equipment or data center cooling systems.

D. PURCHASING DEPARTMENT

The Purchasing Department and procurement managers shall review equipment requests for energy-efficient characteristics and seek energy-efficient and/or green-computing options for new purchases.

All technology procurement evaluations for equipment costing more than \$2,000 shall include an evaluation of energy efficiency and energy consumption costs related to long-term use of the equipment.

When submitting Requests for Quotes (RFQ), the Purchasing Department shall:

- Request the equipment be certified by the US Environmental Protection Agency's (EPA) "ENERGY STAR" program at a Plus 80 rating or higher. Where the cost difference between a technology alternative rated at Plus 80 is less than 10 percent higher than an alternative rated at a lower energy efficiency (all other factors being equivalent), the more efficient alternative should be purchased.
- Recommend laptop computers over full-sized desktop machines. This preference may be mitigated by factors of business use, user productivity, and organizational security policy.
- Flat-panel liquid crystal display (LCD) monitors should be preferred over conventional cathode-ray tube (CRT) monitors.
- Printers that can print on both sides of paper (duplex printing) should be preferred over single-side printers.
- Except in cases of a specific business or security need for the procurement of a dedicated printer assigned to a single individual, departmental management and procurement should encourage the use of networked or shared printers. When

the procurement of a personal/dedicated printer is indicated, procurement should prefer more energy-efficient inkjet printers over laser printers.

- Actively seek and evaluate energy-efficient and “green computing” offerings, noting computer vendors that offer resource-efficient machines designed for eventual recycling.

E. EQUIPMENT RECLAMATION, RECYCLING, AND DISPOSAL

- Staff not in charge of equipment disposal should not throw away computers or other equipment, even if they are non-functional. Staff should contact their IT Department to properly dispose of unused or unusable computer equipment.
- Staff responsible for equipment disposition should use procedures in compliance with the Disposal Policy.
- In cases where the entirety of a machine cannot be reused, the IT Department Staff should seek to salvage and reuse any valuable components.
- CRT monitors that contain hazardous materials must be disposed of in compliance with hazardous materials disposal procedures.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.11, APO10.05, BAI02.05-06, BAI02.09, BAI10.05
GDPR Article 25, 35
HIPAA 164.308(a)(1)(ii)(A), 164.310(b)
ISO 27001 A.11.2
NIST SP 800-37 3.3, 3.5
NIST SP 800-53 AT-3, MA-2, MP-6
NIST Cybersecurity Framework ID.AM-1, ID.AM-5, PR.DS-3
PCI 6.1, 6.4.5

GUEST ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	December 31, 20XX
Approved By	Policy Committee
Effective Date	January 1, 20XX
Current Version	1.0

I. Overview

Computer accounts are the means used to grant access to ABC Company information resources. These accounts provide a means of providing accountability, a key to any computer security program, for information resources usage and restrictions. Specific circumstances may require guests (non ABC Company Staff) to have access to ABC Company Information Resources.

II. Purpose

This policy establishes the rules for the creation, monitoring, control, and removal of guest user accounts.

III. Scope

This policy applies to all individuals who have access to ABC Company's Information Resources.

IV. Policy

Access to ABC Company Information Resources by a guest shall be coordinated through a sponsor. The sponsor will typically have some relationship with the guest. The sponsor will take responsibility for the actions of the guest while they are utilizing ABC Company Information Resources.

Members of the Board of Directors or advisory group members shall be eligible for guest access for the duration of their term. ABC Company Executive Management is allowed to sponsor a guest up to 90 days. Department Heads are allowed to sponsor a guest up to 7 days. The following categories of guests are eligible to be sponsored:

- New Staff waiting for their permanent logon credentials.
- Staff attending orientation or educational events.
- Commercial vendors or suppliers invited to demonstrate their equipment.
- Media such as television, radio, newspapers, and magazines.

- Conference and meeting presenters attending an event sponsored by an ABC Company Department. Participants are eligible for sponsorship only if they are actively participating in the event and not just a member of the audience.

Guest access to Information Resources shall be permitted only after approval from the appropriate sponsor. Guests are allowed to access the Internet, selected printers, and basic Microsoft Office programs. Guests shall not have the ability to:

- Download files from the Internet.
- Modify or install programs or utilities.
- Save files to hard drives.

Guests are subject to the same procedures and security controls used for ABC Company Staff. Sponsors are responsible for ensuring that guests know the procedures and security controls governing access to Information Resources. The IT Department is responsible for assigning temporary IDs to the guest and making records available for audit. It is the responsibility of service providers to determine to what extent guests are eligible to use their services and to authorize service usage as needed.

The IT Department shall implement a wireless network to support wireless access for guests. Procedures shall be established to ensure the guest wireless network cannot connect to ABC Company's in-house network or access company data. The guest wireless network shall meet the security requirements specified in the Wireless Access Policy.

The Chief Security Officer shall ensure:

- The organization has implemented procedures for terminating access when the guest leaves or the time period has expired.
- Procedures assign responsibility for removing IT and/or physical access. Procedures include timely communication of termination actions to ensure that the procedures are appropriately followed.
- Procedures are based upon initial access authorization and subsequent modification of a guest's access to Information Resources.
- Procedures are in place for establishing and modifying guest access to Information Resources. Such procedures shall be formally documented and updated regularly.
- An annual, or more frequent, review of the procedure to grant, modify, and terminate guest access to Information Resources.
- The organization assigns a unique name and/or number for identifying and tracking user identity. Procedures require the user ID to be in a specific format and specify the format to be used. Procedures specify that the unique user ID be used to track guest activity.

- Authentication procedures verify a person or entity seeking access to Information Resources is the one claimed. Policies specify the types of approved authentication mechanisms that are reasonable and appropriate.

All guest accounts created must have an associated request and approval that is appropriate for the ABC Company system or service. All accounts must be uniquely identifiable using the assigned user name.

All default passwords for accounts must be constructed in accordance with the ABC Company Password Policy. All accounts must have a password expiration that complies with the guest sponsor time period and Password Policy.

System Administrators or other designated staff:

- Are responsible for granting, modifying and removing guest accounts when they reach the end of their sponsor period.
- Must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
- Must have a documented process for periodically reviewing existing accounts for validity and ensuring that guest accounts are removed in a timely manner.
- Are subject to independent audit review.
- Must provide a list of accounts for the systems they administer when requested by authorized ABC Company management.
- Must cooperate with authorized ABC Company management investigating security incidents.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 64.308(a)(4)(ii)(B), 164.310(a)(2)(ii), 164.310(a)(2)(iii)
ISO 27001 8.2-3, A.7, A.8.3.3, A.9, A.11
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 AT-3, PS-1, PS-3, PS-7
NIST Cybersecurity Framework ID.RA-6, ID.RM-1, PR.AC-1-2, PR.AC-7, DE.CM-2-3
PCI 6.1, 7.1-3, 8.1, 8.6, 9.1-4, 9.10

HARDWARE AND SOFTWARE MAINTENANCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Maintenance of Information Resources hardware and software is part of F2OnSite's risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

The formal process of maintaining hardware and software ensures that a clearly defined set of procedures is used to document and minimize risks related to Information Systems.

III. Scope

This policy applies to all F2OnSite Staff that use Information Resources.

IV. Policy

This policy identifies the hardware and software maintenance and support arrangements for all standard and non-standard Information Resource servers, network infrastructure equipment, workstations, peripherals, and related software. This policy includes applications and systems that are subject to their own maintenance and upgrade policies. The IT Department will ensure that hardware and software maintenance activities are properly recorded in the Information Systems Log Form.

A. HARDWARE

The IT Department will:

- Ensure that important servers and network infrastructure are covered by on-site warranty agreements from the appropriate vendors with a response time sufficient to meet business needs.
- Arrange for faulty items that are under warranty to be repaired.

- Arrange for repairs or replacement of equipment that is not covered by warranty.

The IT Department will procure and install other types of network and computer hardware including printers, scanners, monitors, keyboards, mice, etc. This ensures:

- The equipment is compatible with existing F2OnSite equipment.
- Centralizes purchasing so the best price is received.
- Equipment is under warranty and maintenance support agreements.
- The equipment is properly configured and has security controls.

B. SOFTWARE

For the purposes of this Policy, software includes:

- Operating systems, virtualization, firmware, and related software.
- Major applications such as order processing, customer relationship management, HR, E-mail, etc. and related databases and interfaces
- Office productivity software including spreadsheets, word processing, presentation, etc.
- Third party applications such as Internet browsers, Adobe Acrobat Reader, media players, Flash Player, etc.
- Security protection software such as firewalls, anti-malware, etc.
- Utilities and other tools

The IT Department shall be responsible for the installation and maintenance of software. The IT Department shall:

- Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry accepted definitions. Update system configuration standards as new vulnerabilities are identified.
- Install and maintain software.
- Maintain software license records.
- Fully test the application and ensure it is compatible with and runs on IT Department standard hardware.
- Where appropriate, subscribe to vendor software maintenance.
- Ensure the software is configured to run at optimum levels.
- Ensure the software and data are fully backed up to ensure systems can be recovered in the event of a failure.
- Updated with critical system patches within 30 days of release. Patches are to be tested before rolling out to production environments.
- Ensure third party vendors work in conjunction with the IT Department.

C. APPROVAL

All departments must seek approval from the IT Department prior to purchasing any special or non-standard hardware, software, or other equipment. IT Department support for non-standard hardware, software, or other equipment will be assessed and agreed on a department-by-department basis.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO09.05, APO10.05, APO11.09, APO13.07, BAI02.05, BAI04.05, DSS04.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(e)(2)(i), 164.314(a)(2)(i)

ISO 27001:2013 4.4, A.11.2.4, A.15.2.1, A.17.1.2

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 MA-2, MA-6

NIST Cybersecurity Framework ID.RA-4, ID.RA-6, PR.AC-2, PR.MA-1, PR.MA-2, DE.DP-2

PCI 8.1, 8.3.2, 9.7, 9.9.3

HEALTH SAFETY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite Staff are an important asset to our organization. The health and safety of F2OnSite Staff must be protected to ensure the continuity of F2OnSite operations.

II. Purpose

The purpose of this policy is to ensure proper controls are implemented and maintained to protect the health and safety of our Staff. In furtherance of this purpose, F2OnSite has established a Health Safety Committee.

III. Scope

This policy applies to all F2OnSite Staff.

IV. Policy

A. HEALTH SAFETY OVERVIEW

This policy specifies actions to be performed to ensure the health and safety of our Staff, clients, service providers, visitors, and other persons. Staff must acknowledge in writing that they have read and understood this policy.

Each F2OnSite Department Head shall prepare customized procedures that support this policy. Such procedures shall be submitted to the Health Safety Committee for review and approval. At a minimum, the Health Safety Committee shall consist of the Risk Management Officer (RMO) and HR Director.

Staff shall be trained on health safety requirements and processes associated with their job duties. Such training shall include interactions with others, use of facilities, and related safeguards.

The Health Safety Committee shall ensure mechanisms exist to monitor and measure compliance with this policy. Within their area of responsibility, each Department Head shall be responsible for enforcing compliance with this policy.

The Health Safety Committee shall implement a system for health safety incident reporting, response, tracking, and resolution.

All Staff are responsible for reporting to the Health Safety Committee any violations of this policy.

B. ENTRY AREAS

Access to F2OnSite facilities shall be controlled. Security personnel at entry points shall conduct non-invasive temperature checks on Staff, clients, service providers, visitors, and other persons. Anyone found to have a temperature over 100 degrees shall be turned away and not permitted access to facilities.

Unless approved by the Health Safety Committee, entry and waiting areas shall not offer magazines, periodicals, and other material as they are difficult to clean and disinfect.

C. PROTECTIVE EQUIPMENT

The Health Safety Committee shall determine the type of personal protective equipment (i.e. masks, gloves, etc.) to be used when Staff, clients, service providers, visitors, and other persons are on-site at F2OnSite facilities. The Health Safety Committee shall ensure Staff are trained on how to properly use and dispose of such equipment.

D. HEALTH SAFETY REMINDERS

Health safety reminders shall be developed by the Health Safety Committee. Such reminders shall be posted in prominent locations and remind personnel of appropriate procedures to be followed.

E. SAFETY PRECAUTIONS

Hand sanitizer dispensers shall be placed at entry points, receptions/lobbies, and at other locations as determined by Department Heads and the Health Safety Committee.

Staff shall be reminded not to touch their face and shall wash their hands with soap and water at least once an hour.

Staff should avoid non-essential travel.

Staff should seek medical attention if they experience one or more of the following symptoms:

- Fever

- Repeated cough
- Shortness of breath or difficulty breathing
- Chills or repeated shaking with chills
- Muscle pain
- Headache
- Sore throat
- Loss of taste or smell

F. PHYSICAL DISTANCING

When on-site at F2OnSite facilities, Staff, clients, service providers, visitors, and other persons shall practice physical distancing and stay at least six feet away from others.

The Health Safety Committee shall establish guidelines to reduce traffic flow, the number of people in lines, at reception areas, etc.

G. SANITIZING PROCEDURES

The Health Safety Committee shall determine appropriate facility sanitizing procedures and frequency. Such procedures to include doors, check-in counters, elevators, restrooms, breakrooms, shared equipment, and other locations as determined by the Health Safety Committee.

H. WORK ENVIRONMENTS

Department Heads shall identify Staff resources needed as well as working arrangements. For example:

- Staff who work in private offices are allowed to be on-site
- Staff who work efficiently when off-site are allowed to work off-site
- Staff who work in common areas are rotated on-site one week and off-site the next week

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM02.03, EDM04.09, APO07.03, APO07.08, APO09.05, APO12.02
GDPR Article 9, 17
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(5)(ii)(A)
ISO 27001:2013 6.1, 7.3, A.7.2, A.11.1, A.12.1, A.18.1
NIST SP 800-37 3.3, 3.4, 3.7
NIST SP 800-53 AT-1, IR-1, PE-3, , PS-1, RA-1
NIST Cybersecurity Framework ID.AM-5, ID.RA-3, PR.AC-2, PR.AT-1, DE.CM-3, RS.RP-1
PCI 8.6, 9.1, 9.3, 9.4, 9.10

HIPAA AND HITECH POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite values its relationships with our health care customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

II. Purpose

The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and Canadian Personal Health Information Protection Act (PHIPA) specify security standards, privacy requirements, and security breach notification procedures. A strong health care compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

III. Scope

This policy applies to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

IV. Policy

HIPAA is designed to protect sensitive health care information through improved security standards and privacy legislation. It defines requirements for collecting, storing, and transmitting patient information. It also identifies compliance guidelines for critical business tasks such as risk analysis, awareness training, audit trail, disaster recovery plans, information access, and encryption.

HITECH requires entities, business associates, vendors of personal health records and related entities to notify individuals when their personal health information is subject to a breach of security. To limit exposure, limited data sets with de-identified data shall be used to disclose only the minimum necessary protected health information.

To meet compliance requirements, F2OnSite shall implement the required information security standards as outlined in the HIPAA Security Rule. The security standards are organized into three major safeguard areas:

- Administrative Safeguards - policies and procedures for day-to-day operations, managing the conduct of employees with access to electronic protected health information (EPHI) as well as managing the selection, development, and use of security controls.
- Physical Safeguards - security measures that protect an organization's electronic information systems, buildings, and equipment from natural hazards, environmental hazards, and unauthorized intrusion.
- Technical Safeguards - security measures that specify how to use technology to protect electronically protected health information and access to such information.

The table below identifies F2OnSite policies and plans that implement and maintain specific Safeguards to meet HIPAA, HITECH, and PHIPA compliance requirements. While larger firms generally have a designated Chief Privacy Officer (CPO), smaller organizations may have a Chief Security Official (MGMT) fulfill these duties. For more information on Business Associates, refer to the Third Party Service Providers Policy.

Security Control	Policy and Plan	Health
Governance	IT Governance Policy Mergers and Acquisitions Policy Terms and Definitions Policy	164.308
Information Security	Privacy Policy Securing Information Systems Policy Security Controls Review Policy	422.112
Risk Management	Business Impact Analysis Risk Assessment Policy Risk Management Policy	45 CFR 164.308 422.504 820.22
Policies and Procedures	Security Policy Security Policy Intro System Security Plan	422.112 422.202
Organization	Audit Policy IT Governance Policy IT Management Policy IT Support Staffing Policy Outsourcing Policy	422.503 ARRA 13408 13404(b) 13405(b)
Asset Management	Data Classification Policy Network Access Policy Software Licensing Policy	21 CFR 11.1(b) 11.1(f)
Human Resources	Acceptable Use Policy Security Awareness & Training Plan Security Awareness & Training Policy Staffing Policy Social Networking Security Policy Third Party Service Providers Policy	21 CFR 820.20b 820.75b 820.25a PHIPA
Physical and Environmental	Personnel Security Policy Physical Access Security Policy Physical Security Policy	164.310

Communications and Operations	Account Management Policy Anti-Malware Policy Backup Policy Bluetooth Policy Data Integrity Policy Data Marking Policy Data Privacy Policy Domain Controller Policy Domain Name System Policy E-commerce Policy Electronic Disposal Policy E-mail Policy Firewall Policy Guess Access Policy Internet Connection Policy Intrusion Detection Policy Logging Policy Mass Communication Policy Network Address Policy Network Configuration Policy Network Documentation Policy Removable Media Policy Router Security Policy Security Monitoring Policy Server Hardening Policy Vendor Access Policy Workstation Security Policy	820-60 820-65
Access Control	Admin Special Access Policy Asset Management Policy Bring Your Own Device Policy Guest Access Policy Identification and Authentication Logical Access Controls Policy Network Access Policy Password Policy Mobile Device Policy Remote Access Policy Securing Information Systems Policy Securing Sensitive Information Policy Smartphone Policy System Update Policy User Privilege Policy Web Policy Wireless Access Policy	422.501 495.346 21 CFR 11.1e 11.10d 11.10k
Acquisition Development and Maintenance	Acquisition and Procurement Policy Application Implementation Policy Approved Application Policy Audit Trails Policy Change Management Policy Encryption Policy Green Computing Policy Hardware and Software Maintenance Patch Management Policy Production Input Output Controls Quality Assurance Policy Secure Development Lifecycle Policy Server Certificates Policy Software Development Policy VPN Policy Web Site Policy	495.348 820.50 820.80
Incident Management	Identity Theft Protection Policy Incident Response Policy Incident Response Plan Reporting Violations Policy	422.128 ARRA 13402

Business Continuity Management	Business Continuity Plan Business Continuity Policy Business Resumption Plan Continuity Communications Plan Dept Continuity of Operations Plan IS Disaster Recovery Plan Resilience Policy	164.308
Compliance	Certification and Accreditation Policy Compliance Policy Electronic Data Retention Policy HIPAA and HITECH Policy	ARRA 13405(a)

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO09.05, APO12.02, APO13.07, DSS04.05, MEA03.01, MEA04.11
 GDPR Article 25, 32
 HIPAA 164.308, 164.310, 164.312, 164.314, 164.316, 164.502, ARRA 13402, 13404, 13405
 ISO 27001:2013 6.1.2, A5, A7.2.2, A8.1.3, A8.2.1, A9-14, A16-18
 NIST SP 800-37 3.4, 3.7
 NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
 NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
 PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

HITRUST POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite has strong relationships with our health care customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

II. Purpose

Security controls and safeguards are part of F2OnSite's risk management process to mitigate, eliminate, and transfer risks that can impact business operations. A strong health care compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

III. Scope

This policy applies to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

IV. Policy

HITRUST's Common Security Framework (CSF) helps organizations create, access, store, and exchange Protected Health Information (PHI) in a safe and secure manner. The CSF is based on health care security regulations, standards, and frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and International Standards Organization (ISO) 27799:2008 Health informatics, information security management in health using ISO/IEC 27002.

CSF consolidates relevant globally recognized standards, regulations, and business requirements into a risk-based approach to security, privacy, and regulatory challenges.

CSF includes Control Categories which contain Control Objectives and Control Specifications.

The table below summarizes F2OnSite policies and plans that implement and maintain specific Safeguards to help meet HITRUST compliance requirements.

Control Category	Policy/Plan
Information Security Management Program	Context and Alignment Policy Cybersecurity Framework Policy Cybersecurity Policy Mergers and Acquisitions Policy System Security Plan Terms and Definitions Policy
Access Control	Access Control Policy Admin Special Access Policy Bring Your Own Device Policy and Technology Clear Desk Policy Database Security Policy Guest Access Policy Identification and Authentication Policy Logical Access Controls Policy Mobile Device Policy Password Policy Portable Computing Policy Remote Access Policy Securing Information Systems Policy Securing Sensitive Information Policy Smartphone Policy System Update Policy User Privilege Policy Wearable Computing Device Policy Web Policy Wireless Access Policy
Human Resources Security	Health Safety Policy Outsourcing Policy Security Awareness and Training Plan Security Awareness and Training Policy Staffing Policy Social Networking Policy Third Party Service Providers Policy

Risk Management	Business Impact Analysis Cybersecurity Policy Cybersecurity Framework Policy Risk Assessment Policy Risk Management Policy
Security Policy	Security Policy
Organization of Information Security	Audit Policy Cloud Service Provider Policy IT Governance Policy IT Management Policy Security Self Assessment Policy
Compliance	Business Associates Agreement Certification and Accreditation Policy Compliance Policy Data Retention Policy Ethics Policy HIPAA and HITECH Policy HITRUST Policy PCI Policy Security Controls Review Policy Software Licensing Policy System Organization Controls SOC2 Policy Vulnerability and Penetration Testing Policy
Asset Management	Acceptable Use Policy Asset Management Policy Data Classification Policy
Physical and Environmental Security	Facility Security Plan Personnel Security Policy Physical Access Policy Physical Security Policy
Communications and Operations Management	Account Management Policy Anti-Malware Policy Backup Plan Backup Policy Bluetooth Policy Capacity and Utilization Policy Configuration and Management Plan Configuration Management Policy Data Analytics Policy Data Integrity Policy Data Marking Policy

	Disposal Policy Documentation Policy Domain Controller Policy Domain Name System Policy E-commerce Policy E-mail Policy Firewall Policy Guess Access Policy Internet Connection Policy Intrusion Detection Policy Logging Policy Mass Communication Policy Network Address Policy Network Configuration Policy Network Documentation Policy Network Security Policy Problem Management Policy Removable Media Policy Router Security Policy Security Monitoring Policy Server Hardening Policy Vendor Access Policy Workstation Hardening Policy Workstation Security Policy
Information Systems Acquisition, Development and Maintenance	Acquisition and Procurement Policy Application Implementation Policy Approved Application Policy Audit Trails Policy Change Management Policy Encryption Policy Green Computing Policy Hardware and Software Maintenance Policy Patch Management Policy Production Input Output Controls Policy Secure Software Development Lifecycle Policy Server Certificates Policy Software Development Policy VPN Policy Web Site Policy
Information Security Incident Management	Identity Theft Protection Policy Incident Response Policy

	Incident Response Plan Reporting Violations Policy
Business Continuity Management	Business Continuity Plan Business Continuity Policy Business Resumption Plan Continuity Communications Plan Department Continuity of Operations Plan IS Disaster Recovery Plan Resilience Policy
Privacy Practices	Data Privacy Policy GDPR EU Privacy and Data Protection Policy Privacy Policy Quality Assurance Policy Web Site Privacy Policy

Note: Policy/Plan names listed above may provide guidance and direction over more than one control category.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO09.05, APO12.02, APO13.07, DSS04.05, MEA03.01, MEA04.11
GDPR Article 25, 32
HIPAA 164.308, 164.310, 164.312, 164.314, 164.316, 164.502, ARRA 13402, 13404, 13405
ISO 27001:2013 6.1.2, A5, A7.2.2, A8.1.3, A8.2.1, A9-14, A16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8, PCI Software Security Framework

IDENTIFICATION AND AUTHENTICATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

By establishing user accountability and rules for access, F2OnSite mitigates the risks related to unauthorized access to electronically stored information.

II. Purpose

This policy defines the security requirements for establishing accounts, enabling access to Information Resources, and ensures the user is properly authenticated to access the information.

III. Scope

This policy applies to Information Resources data owners and security Staff that implement controls to govern access to Information Resources.

IV. Policy

The Chief Security Officer (MGMT) shall ensure that Information Resources are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls on Information Resources.

Data Owners for each information system shall be responsible for ensuring that authorization and account management processes exist for their specific application and that the appropriate people have been assigned the responsibility of creating and maintaining the authorization records. The design and development of the authorization and account management processes shall comply with MGMT security standards.

Department Heads shall submit user access requests to the appropriate Data Owners. As appropriate, Data Owners shall approve or deny such requests for user access privileges.

System Administrators have the responsibility of periodically reviewing user access privileges and notifying the appropriate Data Owners of any access concerns.

The request for Information Resource Authorization shall adhere to the following requirements:

- Access shall be limited to the Information Resources described on the request.
- The Information Resources shall only be used for the purpose stated on the request.
- A new request will be submitted if there are any changes to the stated conditions of access
- The authorization request must be signed by the applicant and approved by the Department Head.

Access to Information Resources is generally established or reviewed under the following conditions:

- A new Staff member requires access to Information Resources.
- A Staff member has a change in job functions.
- A Staff member is terminated or no longer needs access to certain Information Resources.
- A Staff member requires additional access rights.

Requests for a change in access rights (e.g., to grant or disallow access) shall be accomplished by submitting a new request

When a Staff member is transferred or terminated, the Staff member's access to Information Resources must be terminated. The Staff member's records and data, stored locally or in network directories, must be preserved. It is the responsibility of the direct supervisor or manager to contact the Data Owner and the System Administrator when a Staff member is transferred or terminated.

The Data Owner for each information system shall ensure that all user accounts are reviewed and access rights evaluated at least once per year.

User identification and authentication is an access control methodology. At a minimum, F2OnSite uses two-factor authentication with an ID and password to determine a user's identity, ensure it is correct, and establish accountability. User login IDs shall be unique and shall not be shared by Staff members unless special permission is authorized by Executive Management. User selected passwords are required to authenticate the user and grant access to F2OnSite Information Resources.

The Chief Security Officer (MGMT) shall ensure:

- Sensitive authentication data shall not be stored after authorization even if it is encrypted.
- If sensitive authentication data is received, processes shall render all data irretrievable upon completion of the authorization process.
- Processes permit storing of sensitive authentication data if there is a business justification and the data is stored securely.

Access controls shall be implemented to protect Information Resources. Only IT Department approved access control software shall be used to restrict access to Information Resources. Access to security protection systems shall be limited to security administrators and authorized personnel.

Logical access controls may be implemented on applications and databases. These controls shall have the effect of limiting access to data based upon the principle of least privilege.

The number of consecutive attempts to enter an incorrect password shall be limited to prevent password guessing attacks. After a given number of unsuccessful attempts to enter a password, the ID shall be suspended until reset by a system administrator. Please refer to the Securing Information Systems Policy for more information.

If there has been no activity for a given period of time, the system must automatically either blank the screen or use a screen saver, and restrict access. Re-establishment of access may occur after the user has logged back on to the system. Please refer to the Securing Information Systems Policy for more information.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Information Resources data owners and security Staff that implement controls to govern access to Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05

GDPR Article 25, 32

HIPAA 64.308(a)(4)(ii)(B-C), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B-C)

ISO 27001:2013 A.6.2.2, A.7.3, A.9

NIST SP 800-37 3.2, 3.6

NIST SP 800-53 AC-1-2, IA-2, IA-4, IA-5, IA-8

NIST Cybersecurity Framework PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-7, DE.DP-2

PCI 6.3, 6.5.8, 8.1-2, 8.8.2

IDENTITY THEFT PROTECTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Policies and procedures help F2OnSite meet compliance requirements by addressing identity theft issues in a uniform and consistent manner. For example, they dictate the steps to be followed when we receive a notice of address discrepancy from a consumer reporting agency.

II. Purpose

The purpose of the Identity Theft Protection Policy is to establish the rules for the creation, monitoring, control, and maintenance of covered accounts.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's customer information.

IV. Policy

A. PROGRAM COORDINATOR

F2ONSITE has appointed a Program Coordinator of our Identity Theft Red Flags Program. The Program Coordinator SHALL PREPARE AN IDENTITY THEFT RISK ASSESSMENT REPORT TO DETERMINE WHETHER **F2ONSITE** OFFERS OR MAINTAINS COVERED ACCOUNTS AS DEFINED IN THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003 ("FACTA"). AT A MINIMUM, THE RISK ASSESSMENT REPORT SHALL REVIEW THE ACCOUNTS AND SERVICES OFFERED, ASSESS PAST INCIDENTS, DOCUMENT SUSPICIOUS INFORMATION, EVALUATE IDENTITY THEFT DETECTION METHODS, AND ASSESS RESPONSE PROCEDURES.

The Program Coordinator shall design, implement, and maintain policies and procedures implementing identity theft detection procedures, response procedures, and an **IDENTIFY THEFT PROTECTION PROGRAM TO ADDRESS IDENTITY THEFT AND SATISFY THE REQUIREMENTS OF FACTA LEGISLATION. THE IDENTITY THEFT PROTECTION PROGRAM SHALL INCLUDE, BUT NOT BE LIMITED TO,**

SERVICES OFFERED, POLICIES AND PROCEDURES RELATED TO IDENTITY THEFT, RELEVANT RED FLAGS, DETECTION, PREVENTION, AND MITIGATION ACTIONS, AS WELL AS UPDATES TO THE IDENTITY THEFT PROTECTION PROGRAM.

Specific responsibilities that have been delegated to the Program Coordinator include:

- Identifying and assessing the risks of identity theft and discovery of address discrepancies in each relevant area of the Company's operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks and to respond to situations in an appropriate fashion.
- Designing and implementing policies and procedures that are appropriate for the size and complexity of our Company and its operations considering the nature and scope of our activities and the sensitivity of the customer information we collect, store, and share with others.
- Regularly monitoring and testing the policies and procedures for compliance with all applicable law and to determine the effectiveness of our procedure in preventing identity theft.
- Assisting with the selection of appropriate service providers that are capable of maintaining safeguards to protect against identity theft and reviewing service provider contracts to ensure that each maintains appropriate procedures for identifying and responding to situations involving identity theft.
- Evaluating and adjusting this procedure in light of relevant circumstances, including changes to F2OnSite's operations, business relationships, technological developments and/or other matters that may impact the security or integrity of customer information and response to identity theft.

The Program Coordinator is the contact person for law enforcement agencies to communicate possible situations of identity theft. Upon receiving a request for information from any law enforcement agency, the Program Coordinator will:

- Provide the law enforcement agency with his/her name, title, and appropriate contact information, such as a mailing address, e-mail address, telephone number and facsimile number, and notify the law enforcement agency promptly of any modifications with respect to contact information.
- If F2OnSite has identified possible identity theft or becomes aware of an address discrepancy, the Program Coordinator will send a Report to the customer, as necessary, and to the appropriate law enforcement agency that contains:
 1. The name of the individual, entity or organization
 2. The account numbers or, in the case of transactions, the date and type of each transaction
 3. The Social Security Number, taxpayer identification number, passport number, date of birth, address, or other personal identifying information provided by the individual or entity at the time of the transaction.

To assist in compliance with applicable state and federal regulations, the Program Coordinator will audit the Company's Policies and Procedures at least bi-annually to determine if the current system is operating effectively to prevent/detect identity theft and to deal with notice of any address discrepancy. Any modification of the system that the Program Coordinator deems appropriate will be implemented as soon as reasonably possible. As part of the audit program, Company personnel will be encouraged to advise the Program Coordinator of any newly identified risks to customers or to the safety of the Company regarding identity theft. To the extent of any newly identified risk that is discovered, the Program Coordinator is authorized to take appropriate action to address the risk, including assessment, independently or through third parties, of the severity of this risk, and make modifications of the audit system by written instruction to all necessary personnel or through obtaining outside products or services to alleviate the risk.

At least annually, the Program Coordinator will report to management:

1. The effectiveness of the Program
2. Explaining "significant events" involving identity theft and management's response to any incident
3. Providing recommendations for substantive/material changes to the Policies and Procedures due to evolving risks and methods of identity theft.

B. EMPLOYEE MANAGEMENT AND TRAINING

All current employees and new hires, as well as independent contractors who provide services to or that perform services on behalf of F2OnSite, will:

- Be subject to satisfactory reference and consumer/criminal report investigations, where appropriate.
- Only have access to customer information if they have a business reason for seeing it.
- Participate in the Company's privacy policies and information security standards and identity theft and notice of address discrepancy training program and attend education and training seminars on a regular basis, if not otherwise provided for by any independent contractor for its own employees.
- Sign and acknowledge his/her agreement to this procedure.
- Be responsible for protecting the confidentiality and security of the customer information our Company collects and for using the information in accordance with our Policies and Procedures.
- Not be permitted to post passwords near their computers or share passwords with any other person.
- Refer telephone calls or other requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Company's business or are for information that the employee is not authorized to provide.

- Disclose to service providers, marketers or any other parties only that customer information which is necessary to complete a transaction initiated by the customer and/or as permitted by law. If an employee is unsure as to whether a specific disclosure is permitted, he or she will be instructed to check with the Program Coordinator or appropriate manager prior to releasing the information.
- Be required to notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.

When an employee ceases to be employed by the Company, he/she will be required to turn in any keys in his/her possession that provide access to the Company and file cabinets, desks, and offices in the Company; passwords and security codes, if applicable, will be deleted; and employees will not be permitted to take any customer information from the Company.

C. OBTAINING CUSTOMER INFORMATION AND VERIFYING CUSTOMER IDENTITIES

The following procedures will be implemented with respect to obtaining customer information and verifying customer identities:

- Forms utilized by the Company request customer information, such as names, addresses, telephone numbers, birth dates, social security numbers, tax identification numbers, and driver's license and insurance information, to enable the Company to verify the identification of its customers. In addition, customers must sign documentation, including sworn statements in some cases, wherein the customer represents and warrants that he/she is the person identified in the documentation.
- Employees will request to see the customer's driver's license or other form of government-issued identification bearing a photograph to verify the customer's identity and will make a copy of the same to retain in the customer's file. If a customer requests financing in connection with a transaction, the customer will be required to provide employment information and references and must authorize the Company to obtain a credit report, all of which may be utilized to verify the identity of the customer and be used to check for any notice of an address discrepancy. Employees may also request copies of the customer's utility bills, bank or credit card statements and paycheck stubs.
- In the event that customer information provided is conflicting or cannot be verified upon further inquiry, employees shall request additional government-issued documentation evidencing the customer's residence and bearing a photograph or other safeguard (i.e. a social security card, alien identification card, or passport) to enable employees to form a reasonable belief that they know a customer's true identity. When appropriate, employees shall write a summary of the means and results of any measures taken to identify a customer, including the resolution of any discrepancy in the identifying information obtained. Employees will be

instructed to notify the Program Coordinator if customer information still cannot be verified, or if the employees have obtained information regarding an address discrepancy that cannot be explained.

- Paper and electronic records containing customer information and relevant to the Company's identity verification process will be retained by the Company in accordance with federal and state record retention requirements. Upon the expiration of the appropriate retention period, any such records will be disposed of in a secure manner in accordance with the Company's information security standards.

D. INFORMATION SYSTEMS

The following information security standards will be implemented in order to protect customer information collected and maintained by our Company:

- Employees will have access only to that customer information which is necessary to complete their designated responsibilities. Employees shall not have access to or be authorized to provide any other unauthorized person access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of the Company's ordinary business or the scope of an employee's authorization must be directed to the Program Coordinator or designated individuals.
- Access to electronic customer information will be password controlled. Every employee with access to the Company's computer system and electronic records will have a unique password consisting of at least characters, including numbers and letters. Only employees that need to access electronic records will be provided with authorized access.
- All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Any paper records containing customer information must be stored in a deal jacket or folder. Paper records must be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records will be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records will be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors, and service providers shall not be left in an area with insecure customer records.
- Backups of the computers and/or server will be made at least once every day, or at more frequent intervals as deemed necessary. At least once each month the backup information will be verified. Backup disks will be stored in a locked file cabinet.
- Virus protection software shall be installed on computer systems and new virus updates will be checked at regular intervals. All computer files will be scanned at least once each month, or at more frequent intervals as deemed necessary.
- Firewalls and security patches from software vendors will be downloaded on a regular basis.

- All data will be erased from computers, disks, hard drives, or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives will be removed and destroyed. Any paper records will be shredded and stored in a secure area for an authorized disposal/recycling service.
- Employees will log off of all Internet, e-mail and other accounts when not being used. Employees will not be permitted to download any software or applications to Company computers or open e-mail attachments from unknown sources. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator.
- Electronic records will not be stored online and are not accessible from the internet. If customer information is transmitted electronically over external networks, the information will be encrypted at the time of transmittal.
- Neither current nor former employees will be permitted to remove any customer information from the Company, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

E. SELECTION AND OVERSIGHT OF SERVICE PROVIDERS

In order to protect the customer information our Company collects, and to deal with alerts and notices, we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers:

- Compatibility and willingness to comply with the Company's policies and procedures and the adequacy of the service provider's own policies and procedures.
- Records to be maintained by the service provider and whether the company will have access to information maintained by the service provider.
- The service provider's knowledge of regulations that is relevant to the services being provided, including privacy, identity theft, and other consumer protection regulations.
- Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.
- Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions.
- Service and support that will be provided in terms of maintenance, security, and other service levels.
- Financial stability of the service provider and reputation with industry groups, trade associations, and other organizations.
- Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; warranty,

confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract re-negotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage to be maintained by the service provider; and use of the Company's data, equipment, and system and application software.

- The right of the Company to audit the service provider's records, to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider's facilities.

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing the Company's information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer and Company information, to comply with applicable privacy and identify theft regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Company or its customers and to notify the Company to the services provider's corrective action.

Service Providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.

F. IDENTITY THEFT DETECTION

The Program Coordinator will implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information or notices of any address discrepancy and to ensure that employees, independent contractors, and Service Providers are complying with our Company's Policies and Procedures.

Identity theft detection procedures can include:

- Follow Bank Secrecy Act procedures
- Follow Anti-money Laundering procedures
- Follow Customer Identification Program procedures
- Investigated alerts from Consumer Reporting Agency (CRA)
- Inspect application documents
- Inspect identification documents
- Compare identification information to internal information for other similar account holders
- Verify that identification document presented is of the type issued by a government

- For online applications, confirm that IP address is consistent with the applicant's indicated geographic location
- Validate Social Security Number
- Use shared secrets (e.g., the applicant is asked for information only the institution and the applicant knows)
- Review county of residence
- Require multiple confirmations of true identity
- Use of external databases (CRA, public records)
- Procedures exist for changes to account information such as postal address
- On-line access to accounts are locked after a number of invalid signon attempts, written reactivation procedure exists

G. IDENTITY THEFT RESPONSE PROCEDURES

In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator may modify or supplement our Company's Policies and Procedures.

If the Company experiences an identity theft breach, the Program Coordinator will inform management and will take appropriate steps to notify counsel, Service Providers, customers, and the appropriate law enforcement agency of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.

Identity theft response procedures can include:

- Determine whether a suspicious activity report (SAR) should be filed
- When identify theft is detected in an account, investigate the account holder's other accounts for identity theft
- For online account access, if an IP address is not recognized, require the account holder to answer a challenge question
- In the event of failed website or automated telephone authentication, require applicant or account holder to contact a service representative
- When to investigate Red Flag and temporarily suspend account
- When to investigate Red Flag, but do not suspend account
- Monitor the account for evidence of identity theft
- When to contact the applicant or account holder
- Change passwords, security codes, or other security devices that permit access to a covered account
- Reopen the account with a new account number

- When to refuse to open an account
- When to close existing account

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who use Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01
 GDPR Article 25, 30, 32
 HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
 ISO 27001:2013 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18
 NIST SP 800-37 3.4, 3.7
 NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
 NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
 PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

INCIDENT RESPONSE PLAN

I. Introduction

Maintaining the privacy and protection of customers' and employees' personal information is a risk management issue for all organizations. Research continues to show that consumers have widespread distrust of many organizations business practices, including how they collect, use and retain personal information. The increase in identity theft is a concern for all of us. Business systems and processes are increasingly more complex and sophisticated and more and more personal information continues to be collected. Laws and regulations continue to place requirements on businesses for the protection of personal information.

This Incident Response Plan (Plan) is established to help protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. This Plan specifies the process for identifying and reporting an Incident, initial investigation, risk classification, documentation and communication of Incidents, responder procedures, Incident reporting, and training.

This Plan provides a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or Incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the Plan into action.

II. Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to computer related Incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious implications. The Incident Response Team's mission is to prevent damage to our Information Resource assets that can result in loss of revenue, negative impact on our image or reputation, or loss of goodwill. This Plan documents the process by which the Incident Response Team provides an immediate, effective, and skillful response to any unexpected event involving Information Resources.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate, or resolve Information Resource Incidents. The Team is responsible for investigating suspected intrusion attempts or other Incidents in a timely, cost-effective manner

and reporting findings to management and the appropriate authorities as necessary. The Chief Security Officer (MGMT) will coordinate these investigations.

The Incident Response Team will implement various monitoring systems and subscribe to security alert services to keep abreast of relevant threats, vulnerabilities, or alerts from actual Incidents.

A. Incident Response Team Members

Each of the following will assign a primary and alternate member to the appropriate team:

- Business Applications Team
- Credit Payment Systems Team
- Customer Database Team
- Human Resources Team
- Information Privacy Team
- Information Security Team
- Internal Audit Team
- IT Operations Team
- Legal Team
- Location Manager Team
- Network Architecture Team
- Online Sales Team
- Operating System Architecture Team
- Public Relations Team

B. Incident Response Team Roles and Responsibilities

IT Operations Team

- Central point of contact for all IT related Incidents
- Preliminary investigation of Incidents to determine if MGMT needs to be notified
- Notifies MGMT to activate Incident Response Team

MGMT

- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Determines the nature and scope of the Incident with assistance from other Incident Response Team members
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- For direction and guidance, any extortion demands are brought to the attention of executive management

- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the Incident and corrective action taken

Information Security Team

- Contacts qualified information security specialists for advice as needed
- Provides proper training on Incident handling

Information Privacy Team

- Coordinates activities with the MGMT
- Evaluates known or suspected unauthorized access to personally identifiable or other Sensitive Information
- Documents the types of personal information that may have been breached
- Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information
- Assists in developing appropriate communication to impacted parties
- Assesses the need to change privacy policies, procedures, and/or practices as a result of a breach

Network Architecture Team

- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Looks for signs of a firewall breach
- Contacts external Internet service provider for assistance in handling the Incident
- Takes action necessary to block traffic from suspected intruder
- Evaluates unauthorized access to computers, system, network, or other Information Resources
- Evaluates corruption of, or damage to, electronic data

Operating Systems Architecture Team

- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity

Business Applications Team

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the IT Operations Team with any information relating to a suspected breach

- Collects pertinent information regarding the Incident at the request of the MGMT

Online Sales Team

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the IT Operations Team with any information relating to a suspected breach
- Collects pertinent information regarding the Incident at the request of the MGMT

Internal Audit Team

- Reviews systems to ensure compliance with information security policy and controls
- Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
- Reports any system control gaps to management for corrective action

III. Incident Response Team Notification

The IT Operations Team will be the central point of contact for reporting computer Incidents or intrusions. The IT Operations Team will notify the MGMT.

All computer security Incidents must be reported to the MGMT. A preliminary analysis of the Incident will take place by the MGMT and that will determine whether Incident Response Team activation is appropriate.

An Incident Response Form shall be used to identify incidents, classify, and document actions taken.

A. Examples of Incidents

There are many types of computer Incidents that may require Incident Response Team activation. Some examples include:

- Loss of laptop containing sensitive information
- Breach of Personal Information
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak

Many security Incidents, such as isolated occurrences of computer viruses, are easily handled via well-established procedures (especially in larger companies), and do not justify calling out the entire Incident Response Team. This Plan describes the criteria used to classify the severity of security Incidents, and those severities that result in Plan activation.

B. Risk Assessment Classification

Incidents should usually be grouped into a few different risk classification or severity levels, with broad sets of criteria for each level. For example:

- **Severity 1** – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses easily handled by antivirus software.
- **Severity 2** – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.
- **Severity 3** – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.
- **Severity 4** – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.
- **Severity 5** – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

In this example, Incidents of Severity 3, 4, and 5 would result in Plan activation, while Incidents of Severity 1 and 2 would be handled without Incident Response Team involvement.

C. Incident Declaration

When an Incident requiring Plan activation occurs, a formal Incident is declared. The IT Operations Team notifies the MGMT that an Incident has been detected. The MGMT is then responsible for confirming the IT Operations Team findings and analysis and, if appropriate, activates the Incident Response Team.

IV. Response Procedures

Response procedures can be described at two levels of detail in the Plan. The first level of detail is a set of general guidelines that describes the principal phases of Incident response, and what happens during each phase. Every Plan should include this level of detail. The second level of detail is a set of step-by-step response procedures, specific to individual Incident types (e.g., procedure(s) for handling virus Incidents, procedure(s) for handling hacker break-ins, etc.). These procedures will generally be created over time, and can be added to the Plan in appendices as they are developed.

A. Incident Response Phases

There are five principal phases of Incident response, shown below. The general procedures to be followed in each phase are described in the appendices.

- **Alert Phase** - The alert phase is the process of learning about a (potential) security Incident, and reporting it to the Incident Response Team. Alerts may arrive from a variety of sources including: monitoring systems, Staff reporting of an event, firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc. The Incident Response Team is usually notified by providing a “hotline” telephone number that is reachable 24 hours a day, 7 days a week.
- **Triage Phase** - The triage phase is the process of examining the information available about the Incident to determine first if it is a “real” Incident, and second, if it is, its severity. The Incident Response Team Manager usually does this, with assistance from the permanent team members. If the Incident’s severity warrants, the Incident Response Team management advisory board will also be alerted in this phase. The board must do two important things in this phase: A decision to “pursue” or “protect” must be made. In other words, does the company want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to stop the Incident and restore normal operations? This decision must be made before response begins, because it influences how the response will happen. Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the Incident.
- **Response Phase** - In the response phase, the Incident Response Team gathers evidence (audit trails, log files, contents of files, etc.). If the “pursue” option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court; the team may need specialized technical assistance and advice from a third party to do this successfully. Once evidence has been gathered, it is analyzed to determine the cause of the Incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the Incident. An assessment is also made of how far the Incident has spread, i.e., which systems are involved, and how badly have they been compromised.
- **Recovery Phase** - The recovery phase begins once the response phase has been completed (there may at times be some overlap). In this phase, the Incident Response Team restores the systems affected by the Incident to normal operation. This may require reloading data from backup tapes, or reinstalling systems from their original distribution media. Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the Incident. They are also tested to make sure they will function correctly when placed back into production.
- **Maintenance Phase** - The maintenance phase is also called “lessons learned.” In this phase, the Incident and response are reviewed to determine the parts of the Plan that worked correctly, and the parts that need improvement. The areas in which improvement is needed are then corrected, and the Plan updated accordingly. Other

areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

B. Issues

Five important issues that must be addressed by the above steps include:

1. The systems impacted and the extent of damage or breach
2. How the breach occurred
3. Steps taken to mitigate or remedy the situation
4. Suspects (internal or external)
5. Evidence that exists or needs to be preserved

V. Breach of Information Security

A. Overview

This Plan outlines steps our organization will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a customer or employee of our organization.

In addition to the internal notification and reporting procedures outlined below, credit card companies require us to immediately report a security breach, and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Specific steps are outlined in the Appendix. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of personal information as covered in the Appendix.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the organization collects about an individual is likely to be considered personal information if it can be attributed to an individual.

For the purposes of this Plan, and as defined by the Federal Trade Commission (FTC), personal information is defined as “individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) credit or debit card information, including card number, expiration date, and security code; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies

an individual consumer; or (i) any information that is combined with any of (a) through (h) above.”

B. Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

F2OnSite must identify and document all systems and processes that store or utilize personal information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The business area and the IT development group must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize personal information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

C. Data Owner Responsibilities

Data owners responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between the company and any third party involved with a privacy breach affecting the organization’s data.

All data owners must report any suspected or confirmed breach of personal information on individuals to the MGMT immediately upon discovery. This includes notification received from any third-party service providers or other business partners with whom the organization shares personal information on individuals. The MGMT will notify the Chief Privacy Officer (CPO) and data owners whenever a breach or suspected breach of personal information on individuals affects their business area.

Note: For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the IT Operations Team will act as a central point of contact for reaching the MGMT and CPO.

The MGMT will determine whether the breach or suspected breach is serious enough to warrant full Plan activation (See “Incident Response” section.) The data owner will assist in acquiring information, preserving **evidence**, and providing additional resources as deemed

necessary by the CPO, MGMT, Legal or other Incident Response Team members throughout the investigation.

D. Location Manager Responsibilities

Location managers are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal information. If a breach or suspected breach of personal information occurs in their location, the location manager must notify the IT Operations Team immediately and open an Incident report. (See “Incident Response” Section, IT Operations Team.)

Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of personal information on an individual.

E. When Notification Is Required

The following Incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.
- An intruder has broken into database(s) that contain personal information on an individual.
- Computer equipment such as a workstation, laptop, mobile device, or other electronic media containing personal information on an individual has been lost or stolen.
- A department or unit has not properly disposed of records containing personal information on an individual.
- A third-party service provider has experienced any of the Incidents above, affecting the organization’s data containing personal information.

The following Incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organization can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

- The organization is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The organization determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.
- An intruder accessed files that contain only individuals’ names and addresses.

- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Appendix A - Incident Response Notification

A. Escalation

1. FIRST LEVEL

Chief Security Officer (MGMT)
Director of IT
IT Audit Director
Network Architecture Manager
Online Sales Director

2. SECOND LEVEL

Chief Privacy Officer (CPO)
Chief Audit Executive

B. Internal Contact Auxiliary Members (as needed)

Business Client Systems Manager
Management of Client Department Affected by Incident
Risk Management
Legal
Loss Prevention
Public Relations

C. External Contacts (as needed)

Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Communications Carriers (local and long distance)
Business Partners
Insurance Carrier
External Response Teams as applicable (CERT Coordination Center, etc.)
Law Enforcement
Local Police Force (jurisdiction determined by crime)
Federal Bureau of Investigation (FBI) (especially if a federal interest computer or a federal crime is involved)
Secret Service

D. Notification Order

IT Operations Center (central point of contact)
Chief Security Officer (MGMT)

Information Security Team
 Information Privacy Team
 Appropriate Client Systems Manager
 System Administrator(s) of area affected by Incident
 Manager of area affected by Incident
 Customer Database Manager
 Payment Systems Manager
 Legal Counsel
 Public Relations
 Online Sales Manager
 Employee Systems Manager (where appropriate)
 Network Architectures Manager
 Internal Auditing
 Risk Management (where appropriate)
 Loss Prevention (where appropriate)
 Executive VP and Director of IT (When nature and impact of Incident has been determined)
 Chief Audit Executive
 Business Partners (if connection/data has been compromised; avoid downstream liability)
 Human Resources

Appendix B - Incident Response Team Members

Department	Member	Office Phone	Cell	Home Phone	E-Mail
IT Operations Team					
	Primary				
	Alternate				
Information Security Team					
	Primary				
	Alternate				
Information Privacy Team					
	Primary				
	Alternate				
Network Architecture Team					
	Primary				
	Alternate				

Operating System Architecture Team

Primary

Alternate

Business Applications Team

Primary

Alternate

Online Sales Team

Primary

Alternate

Internal Audit Team

Primary

Alternate

Customer Database Team

Primary

Alternate

Credit Payment Systems Team

Primary

Alternate

Legal Team

Primary

Alternate

Appendix C - Legislation

The following are selected United States laws and regulations relating to the breach of personal information about an individual. This Appendix should not be considered a complete list.

A. U.S. Security Breach/Breach Notification Laws

In the event of a data breach, U.S. states and industry-specific laws and standards require notice to be provided to the affected individuals. Compliance with federal industry-specific requirements may satisfy state breach notification requirements. Laws are generally based on the state of residence of the individual whose data was compromised, not by the company's place(s) of business.

Many states have enacted security breach/data breach laws and regulations. An updated list can be found on the web site of the National Conference of State Legislators <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

For example, on July 1, 2003, California Senate Bill 1386 became Civil Code 1798.82. The law requires companies that do business in California and own or license computerized data containing unencrypted personal information, to notify California residents of any security breach of their unencrypted personal information where the information was, or is reasonably believed to have been, acquired by an unauthorized person. Note: Be prepared to identify and separate, if necessary, California residents from other records in databases containing personal information on individuals.

Contact the Office of the Attorney General of the appropriate state. Have the following information ready:

- Date(s) of breach.
- Date(s) of discovery of breach.
- Date(s) notice provided to consumers.
- If notification was delayed due to a law enforcement investigation.
- Type of personal information involved in the breach.
- Brief description of the breach including number of records, accounts, individuals compromised.
- Type of breach (e.g. unintended disclosure, hacking/malware, payment card fraud, insider, physical access, portable/mobile device, stationary device).
- Location of breached information (e.g. laptop, desktop, network server, e-mail, portable/mobile device).
- Law enforcement agency notified including the report number (if a police report was filed).

B. Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act” or GLB Act, includes provisions to protect consumers’ personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to “financial institutions”, which include not only banks, securities firms and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or

safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional “financial institutions” are regulated by the FTC.

The Financial Privacy Rule governs the collection and disclosure of customers’ personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions. The Rule requires the organization to consider all areas of its operations including employee management and training; information systems; and managing system failures. Effective security includes the prevention, detection and response to attacks, intrusions or other system failures. Specific considerations include maintaining up-to-date and appropriate programs and controls by following a written contingency plan to address any breaches of nonpublic personal information and notify customers if their personal information is subject to loss, damage, or unauthorized access.

The Pretexting provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as “pretexting.”

The Privacy Rule took effect on November 13, 2000 and compliance on July 1, 2001. The Safeguard Rule was effective on May 23, 2003.

C. Health Insurance Portability and Accountability Act (HIPAA)

The primary focus of HIPAA was to improve the health insurance accessibility to people changing employers or leaving the workforce. It also addressed issues relating to electronic transmission of health-related data in Title II, Subtitle F of the Act entitled “Administrative Simplification”. The administrative simplification provisions include four key areas:

- National standards for electronic transmission
- Unique health identifiers for providers, employers, health plans and individuals
- Security Standards
- Privacy Standards

The HIPAA Security Standards require a covered entity to implement policies and procedures to ensure:

- The confidentiality, integrity, and availability of all electronic protected health information
- Protect against any reasonably anticipated threats or hazards to the security of such information
- Protect against any reasonably anticipated uses or disclosures that are not permitted

Within this context, HIPAA requires a covered entity to implement policies and procedures to address security Incidents. A security Incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security Incidents; mitigate, to the extent practicable, harmful effects of security Incidents that are known to the covered entity; and document security Incidents and their outcomes.

The HIPAA security standards were effective on April 21, 2003. The compliance date for covered entities is by April 21, 2005 and April 21, 2006 for small health plans.

D. Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

HITECH specifies the following notification requirements: The covered entity must notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a breach:

- Written notice of the breach sent via first class mail or e-mail (if the individual's preference).
- If more than 500 individuals have unsecured PHI disclosed, additional notice provided immediately to the Secretary of Health and Human Services and to prominent media outlets in the state where the individual resides.
- Business associates notify the covered entity if the associate experiences unauthorized disclosures of unsecured PHI. The covered entity notifies affected individuals within 60 calendar days after the unauthorized disclosure is discovered.

E. General Data Protection Regulation (GDPR)

Article 33 – Notification of a personal data breach

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data

breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification shall at least:

- (a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) Describe the likely consequences of the personal data breach;
- (d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34 - Communication of a personal data breach to the data subject.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

The communication to the data subject shall not be required if any of the following conditions are met:

- (a) The controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- (b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;

(c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph above are met.

Appendix D - Payment Card Standards

A. Requirements

The PCI Data Security Standard was the result of a joint initiative by VISA, MasterCard, American Express, Discover, Diners Club, and JCB to create a single security standard for storing and transmitting sensitive customer information.

The PCI Data Security Standard applies to all members, merchants, and service providers that store, process or transmit cardholder data. Failure to comply with the standards could result in a merchant being subjected to a fine or the loss of access to the credit card networks.

Refer to F2OnSite's PCI Policy for more information on PCI requirements.

B. On-site reviews

Certain merchants, including e-commerce merchants, are required to have an onsite review carried out annually. Any other merchant can also be subjected to an onsite review at the discretion of the payment card institution. The review can be carried out either by the merchant's internal audit function or an independent assessor acceptable to the payment card institution.

C. Self-Assessments

The credit card companies recommend that a Self-Assessment be carried out on an annual basis. For a copy of the Payment Card Industry Self-Assessment Questionnaire, see https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

D. PCI Data Security Standard Plan

Implement an incident response plan. Be prepared to respond immediately to a system breach.

E. MasterCard Specific Steps

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100. In Canada, notify the MasterCard® Global Service™ emergency services via telephone at 1-800-622-2774.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail, to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with the complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues, until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs
2. Distribute the account number data to its respective issuers.

F. Visa U.S.A. Specific Steps

(Excerpted from Visa U.S.A. Cardholder Information Security Program (CISP), What To Do If Compromised, 3/8/2004). Refer to documentation online at http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf.

In the event of a security breach, the Visa U.S.A. Operating Regulations require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the Visa U.S.A. Cardholder Information Security Program. If Visa U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa U.S.A. may require immediate corrective action.

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in Visa programs.

Visa has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, Visa may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.

G. Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.
2. To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
 - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
 - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
 - Preserve logs and electronic evidence.
 - Log all actions taken.
 - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
3. Be on HIGH alert and monitor all Visa systems. Alert all necessary parties, including:
 - Internal information security group and Incident Response Team, if applicable
 - Legal department
 - Merchant bank
 - Visa Fraud Control Group at (650) 432-2978 in the U.S. or Visa Canada Risk Management at 416-860-3090 in Canada.
 - Local FBI Office U.S. Secret Service, or RCMP local detachment, if Visa payment data is compromised.
4. Provide the compromised Visa account to Visa Fraud Control Group at (650) 432-2978 within 24 hours or Visa Canada Risk Management at 416-860-3090 in Canada.
5. Account numbers must be securely sent to Visa as instructed by Visa. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to Issuers and ensure the confidentiality of entity and non-public information.
6. Requirements for Compromised Entities - All merchant banks must:

- Within 48 hours of the reported compromise, proof of Cardholder Information Security Program compliance must be provided to Visa.
- Provide an Incident report document to Visa within four business days of the reported compromise
- Depending on the level of risk and data elements obtained the following must be completed within four days of the reported compromise:
 - Undergo an independent forensic review
 - A compliance questionnaire and vulnerability scan upon Visa's discretion

H. Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at (650) 432-2978. Canada merchants contact Visa Canada Risk Management at 416-860-3090.
2. Participate in all discussions with the compromised entity and Visa USA, or if we are a merchant in Canada with Visa Canada.
3. Engage in a Visa approved security assessor to perform the forensic investigation
4. Obtain information about compromise from the entity
5. Determine if compromise has been contained
6. Determine if an independent security firm has been engaged by the entity
7. Provide the number of compromised Visa accounts to Visa Fraud Control Group or Visa Canada Risk Management within 24 hours
8. Inform Visa of investigation status within 48 hours
9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"
10. Ensure that entity has taken steps necessary to prevent future loss or theft of account information, consistent with the requirements of the Visa USA Cardholder Information Security Program

I. Forensic Investigation Guidelines

Entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise. The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk.
2. Number of accounts at risk, identify those stored and compromised on all test, development, and production systems
3. Type of account information at risk
4. Account number
5. Expiration date
6. Cardholder name
7. Cardholder address

8. CVV2
9. Track 1 and Track 2
10. Any data exported by intruder
11. Perform Incident validation and assessment.
12. Establish how compromise occurred
13. Identify the source of compromise
14. Determine timeframe of compromise
15. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections.
16. Determine if compromise has been contained.
17. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
18. If applicable, review VisaNet endpoint security and determine risk.
19. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.
20. Perform remote vulnerability scan of entity's Internet facing site(s).

J. Visa Incident Report Template

This report must be provided to Visa within 14 days after initial report of Incident to Visa. The following report content and standards must be followed when completing the Incident report. Incident report must be securely distributed to Visa and Merchant Bank. Visa will classify the report as "Visa Secret".

- I. Executive Summary
 - a. Include overview of the Incident
 - b. Include Risk Level (High, Medium, Low)
 - c. Determine if compromise has been contained
- II. Background
- III. Initial Analysis
- IV. Investigative Procedures - Include forensic tools used during investigation
- V. Findings
 - a. Number of accounts at risk, identify those stored and compromised
 - b. Type of account information at risk
 - c. Identify ALL systems analyzed. Include the following:
 - i. Domain Name System (DNS) names
 - ii. Internet Protocol (IP) addresses
 - iii. Operating System (OS) version
 - iv. Function of system(s)
 - d. Identify ALL compromised systems. Include the following:

- i. DNS names
 - ii. IP addresses
 - iii. OS version
 - iv. Function of system(s)
- e. Timeframe of compromise
- f. Any data exported by intruder
- g. Established how and source of compromise

- h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.).
- i. If applicable, review VisaNet endpoint security and determine risk.
- VI. Compromised Entity Action
- VII. Recommendations
- VIII. Contact(s) at entity and security assessor performing investigation

K. Discover Card Specific Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from Discover Card.

L. American Express Specific Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S. and (800) 876-9786 (Option 2) in Canada.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from American Express.

Appendix E - Incident Response Team Procedures

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

A. IT Operations Team

Contacts	Office Phone	Hotline	E-Mail
Primary:			
Alternate:			

1. The IT Operations Team will serve as a central point of contact for reporting any suspected or confirmed breach of personal information on an individual. The following information will be collected by the IT Operations Team
 - Date and time reported
 - Staff member reporting Incident
 - Date and time of Incident
 - Description of Incident (e.g. lost laptop, unauthorized access, virus, etc.)
 - Steps taken by person/department reporting Incident
 - Other relevant information
2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the IT Operations Team will open a Priority Incident Request. This will begin an automated paging process to immediately notify the MGMT.
3. The IT Operations Team will page the primary and secondary contacts in the Information Security Team. The IT Operations Team advises that a breach or suspected breach of personal information on an individual has occurred. After the Information Security Team analyzes the facts and confirms that the Incident warrants Incident response team activation, the Incident Request will be updated to indicate **“Incident Response Team Activation – Critical Incident”**.

B. Chief Security Officer (MGMT)

Contacts	Office Phone	Cell	E-Mail
Primary: Chief Security Officer			
Alternate: Information Security Manager			

1. When notified by the IT Operations Team, the MGMT performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the Incident.

2. Informs the Legal Department and the Chief Privacy Officer that a possible privacy breach has been reported and provides them an overview of the situation.
3. Contacts the individual who reported the problem.
4. Identifies the systems and type(s) of information affected and determines whether the Incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
5. Reviews the preliminary details with the Legal Department and the Chief Privacy Office.
6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the IT Operations Team and advise them to update the Incident Request with "Incident Response Team Activation – Critical Security Problem".
7. Notify the Public Relations Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.
8. The Information Security Team is responsible for documenting all details of an Incident and facilitating communication to executive management and other auxiliary members as needed.
9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
10. Contact appropriate Incident Response Team members and First-Level Escalation members.
11. Identify and contact the appropriate Data Owner affected by the breach. In coordination with the Legal Department, Information Privacy Team and Data Owner, determine additional notification requirements (e.g., Human Resources, external parties).
12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Legal Department, Information Privacy Team and Data Owner to review contract terms and determine next course of action.
13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.
14. Determine the type of personal information that is at risk, including but not limited to: Name, Address, Social Security Number/Social Insurance Number, Account number, Cardholder name, Cardholder address, Medical and Health Information
15. If personal information is involved, have the Data Owner determine who might be affected. Coordinate next steps with the Legal Department, Information Privacy Team and Public Relations (e.g., individual notification procedures).
16. Determine if an intruder has exported, or deleted any personal information data.
17. Determine where and how the breach occurred.
 - a. Identify the source of compromise, and the timeframe involved.

- b. Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.
 - c. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
18. Take measures to contain and control the Incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls. Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
- a. Do not access or alter the compromised system.
 - b. Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
 - c. Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.
19. Monitor systems and the network for signs of continued intruder access.
20. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.
21. Note: Visa has specific procedures that must be followed for evidence preservation.
22. Notify the CPO in coordination with the Legal Department as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.
23. If Protected Health Information (PHI) is involved, follow the additional steps outlined under Appendix C – U.S. Privacy Legislation, Health Information Technology for Economic and Clinical Health (HITECH) Act.
24. If credit cardholder data is involved, follow additional steps outlined under Appendix D – Payment Card Standards. Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security Incidents and the suspected or confirmed compromise of cardholder data. **Reporting is typically required within 24 hours of compromise.**
25. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the company.

C. Information Privacy Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. Coordinates activities with the MGMT.
2. Documents the types of personal information that may have been breached.
3. Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information.
4. Assists in developing appropriate communication to impacted parties.
5. Coordinates with the Public Relations Team.
6. Assesses the need to change privacy policies, procedures, and/or practices as a result of a breach.

D. Network Architecture Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. When notified by the MGMT that the Incident Response Team is activated, provide assistance as determined by the details of the potential breach.
2. Review firewall logs for correlating evidence of unauthorized access.
3. Implement firewall rules as needed to close any exposures identified during the investigation.

E. Operating System Architecture Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. Ensure all service packs and patches are current on mission-critical computers.
2. Ensures backups are in place for all critical systems.

3. Examines system logs of critical systems for unusual activity.

F. Business Applications Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. Monitors business applications and services for signs of attack.
2. Reviews audit logs of mission-critical servers for signs of suspicious activity.
3. Contacts the IT Operations Team with any information relating to a suspected breach.
4. Collects pertinent information regarding the Incident at the request of the MGMT.

G. Online Sales Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. The Online Sales Team will serve as the primary contact for the Online Sales Department. Online Sales Team support is available 24x7 and should be contacted using the above information.
2. When notified by Information Security Team that the Incident Response Team has been activated, the Online Sales Team will collect pertinent information regarding the Incident from the MGMT and determine the appropriate systems involved. If notification of a possible breach of information on an individual comes from any other source (a customer, an individual outside the organization), refer the caller to the IT Operations Team to begin the official Incident response notification process.
3. Online Sales Team, using the information gathered from the sources listed in item 2, will begin by inspecting Web server logs and operating system logs (e.g. Windows event logs, UNIX syslogs). They will look for suspicious activity that may suggest the application interface to processing systems was compromised. From there they will look at the operating system level to ensure that servers were not compromised and used as a pass-through into the backend network. This will also be done by checking event logs, looking at the network for abnormal connections, inspecting the registry for non-standard entries, looking at the running process list for any abnormal executing processes, etc.
4. Due to the sensitivity of a security breach, the Online Sales Team will only notify and communicate with the following management/groups: XXX.
5. Online Sales Team will keep persons informed until it can be confirmed or denied that the online sales systems were compromised.

H. Internal Audit Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. Reviews systems to ensure compliance with information security policy and controls.
2. Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches.
3. Reports any system control gaps to management for corrective action.

I. Customer Database Team

IT Customer Database Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			
Data Owner Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

Notification Steps

1. If the Customer Database Team or Data Owners hear of or identifies a privacy breach, contact the IT Operations Team to ensure that the MGMT and other primary contacts (e.g. CPO) are notified.
2. The Customer Database Team and Data Owner will assist the MGMT as needed in the investigation.
3. IT Customer Database contact notifies the IT Contractor Liaison (if warranted).
 - Monitor access to customer database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).
 - Identify individuals whose information may have been compromised. An assumption could be "all" if an entire table or file was compromised.
 - Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.

- Upon request from the MGMT, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

J. Credit Payment Systems Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. If notified of a privacy breach by a business area directly, open an Incident request with the IT Operations Team to activate the Plan for a suspected privacy breach.
2. When notified by Information Security Team that the Incident Response Team has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of Incident.
 - a. Determine the type of personal information breached.
 - i. Current credit card customers
 - ii. New credit card applications
 - iii. Personal check authorizations
 - b. Determine data sources and method of breach (hardcopy, electronic)
 - c. Determine method of breach if possible.
 - d. Identify additional resources needed to complete investigation
3. Determine the scope of the breach.
 - a. Time Frame
 - b. Specific Data Elements
 - c. Specific Customers
4. Take necessary steps to prevent additional compromise of personal information about individuals.
5. Report all findings to the Plan Team.
6. Within 24 hours of notification of an account number compromise, contact the appropriate card companies:
 - a. Visa Fraud Control Group
 - b. MasterCard Compromised Account Team
 - c. Discover Fraud Prevention
 - d. American Express Merchant Services
7. Act as liaison between the card companies, MGMT, and Legal.
8. Ensure credit card companies' specific requirements for reporting

K. Legal Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

On-going:

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to our clients the effect that any enacted legislation may have on them.
2. Be cognizant of major contracts which the organization enters that may have an impact or effect on our customers, employees, and other data.
3. Be aware of other companies' privacy policies that may affect our organization and affiliates.

When a Privacy Breach Occurs:

1. After confirmation that a breach of personal information on individuals has occurred, notify the Chief Legal Counsel
2. Coordinate activities between business area and other departments (e.g., Human Resources, if necessary).
3. If necessary, notify the appropriate authorities (e.g., Federal Trade Commission (FTC)/RCMP, the relevant privacy office, etc.)
4. Coordinate with Public Relations on the timing and content of notification to individuals.
5. If the Information Security Office determines that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.
6. Notification to individuals may be delayed until the MGMT is assured that necessary measures have been taken to determine the scope of the breach and properly investigated.
7. Follow approved procedures for any notice of unauthorized access to personal information about individuals.
8. Notification to individuals should be timely, conspicuous, and delivered in any manner that will ensure the individual receives it. Notice should be consistent with laws and regulations the organization is subject to. Appropriate delivery methods include written notice, e-mail notice, and substitute notice (conspicuous posting of the notice on the online sales website and/or notification to major media).

Items to consider including in notification to individuals:

- A general description of the Incident and information to assist individuals in mitigating potential harm, including a customer service number, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit

reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

- Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report Incidents of suspected identity theft.
- Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft, and encourage the individual to report any suspected Incidents of identity theft to the FTC. Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected Incidents of identity theft.
- Inform each individual about the availability of online guidance regarding measures to protect against identity theft. Encourage the individual to report any suspected Incidents of identity theft to the local law enforcement agency.

L. Human Resources Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. If notified of a privacy breach affecting employee personal information, open an Incident request with the IT Operations Team to activate the Plan for suspected privacy breach.
2. When notified by the Information Security Team that the Incident Response Team has been activated for a breach of information on an individual, perform a preliminary analysis of the facts and assess the situation to determine the nature of the Incident.
3. Work with the IT Operations Team, MGMT, CPO and business area to identify the extent of the breach.
4. If appropriate, notify the business area that a breach has been reported and is under investigation.
5. Work with the business area to ensure there is no further exposure to privacy breaches.
6. Work with the MGMT, CPO and Legal Department to determine if the Incident warrants further action.

M. Public Relations Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

On-going:

1. Monitor consumer privacy issues and practices of other companies.

2. Monitor consumer privacy breaches of other companies and how they respond.
3. Keep generic/situational talking points current.

When Privacy Breach Occurs

1. After confirmation that a breach of personal information about individuals has occurred, notify the Public Relations Director.
2. Coordinate with the CPO and Legal on the timing, content and method of notification. Prepare and issue press release or statement, if needed.
3. Vehicles for communicating include:
 - a. News wire services
 - b. Online Sales web site – Post statement on home page or conspicuous location of web site.
 - c. Internal Website – If appropriate for breach of employee information
 - d. E-mail
 - e. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
 - i. Appoint appropriate spokesperson
 - ii. Prepare statement and, if necessary, potential Q & A.
 - iii. Coach spokesperson on statement and potential Q & A.
 - iv. Invite select media to attend and cover organization's proactive message.
 - v. Use conference as a platform for communicating who the breach involves, what the organization is doing to correct breach, how it happened and the organization's apology but reassurance of its privacy policies
4. Prepare appropriate response to media, customer, and/or employee; and have the CPO and Legal Department approve prior to distribution.
5. Proactively respond to media inquiries, if necessary.
6. Monitor media coverage and circulate accordingly.

N. Location Manager Team

Contacts	Office Phone	Cell	E-Mail
Primary:			
Alternate:			

1. If the Location Manager becomes aware of or identifies a privacy breach, contact the IT Operations Team to ensure that the MGMT and other primary contacts are notified.
2. The Location Manager will secure the area of the breached information (e.g. computer room, data center, records room).
3. The Location Manager will assist the MGMT as needed in the investigation.

4. The Location Manager will keep the MGMT updated on appropriate investigation information gathered.

Appendix F - Security Breach/Data Breach Resources

A. Data Breach Notification and Response Services

The following service providers help provide forensic investigation, notification, and call center services:

- AllClear ID (877) 441-3009
- CSIdentity (aka CSID) Data Breach Mitigation Services (855) 890-2743
- Equifax Data Breach Services (866) 510-4211 or psol@equifax.com
- Experian Rapid Response Hotline: (866) 751-1323 or databreachinfo@experian.com
- ID Experts (971) 242-4775
- Kroll Data Breach Response, forensics, call center (877) 300-6816

B. Credit/Monitoring Services

F2OnSite has chosen Experian's ProtectMyID service that offers free credit monitoring and identity theft protection. Experian is a leading global information services company that helps individuals understand and keep track of their credit report, as well as monitor for and resolve identify theft. For more information visit <https://www.experian.com/consumer-products/protect-my-id.html>.

Appendix G – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Incident Response Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

INCIDENT RESPONSE POLICY

Policy Area	IT Policy Library
Approved Date	December 31, 20XX
Approved By	Policy Committee
Effective Date	January 1, 20XX
Current Version	1.0

I. Overview

This Policy governs F2OnSite's detection, response, documentation, and reporting of Incidents affecting Information Resources. Incidents include, but are not limited to, unauthorized access, theft, intrusion, misuse of data, other activities contrary to F2OnSite's Acceptable Use Policy, denial of service, corruption of software, computer, and electronic communication-based events.

II. Purpose

This policy is established to protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. This policy establishes an incident Response Team and the process for identifying and reporting an incident, initial investigation, risk classification, documentation and communication of Incidents, responder procedures, incident reporting, and training.

III. Scope

This policy applies to the Risk Management Officer, Chief Security Officer, Executive Management, Director of IT, and Security Staff.

IV. Policy

The Chief Security Officer (MGMT) shall ensure:

- The Risk Management Officer (RMO) is aware of risks related to Information Resources and any changes to Information Resources are communicated to the RMO so that appropriate risk analysis and risk treatment controls can be implemented.
- Procedures and processes identify and respond to suspected or known incidents, mitigate them to the extent practicable, measure harmful effects of known

incidents, document incidents and their outcomes, collect evidence, and provide appropriate reporting to F2OnSite management.

- Incident response procedures list examples of security incidents and the appropriate responses for each.
- An Incident Response Team has been assembled to receive notice of Incidents and manage the process of investigating, responding to, and reporting of the incident.

A. ESTABLISHMENT OF AN INCIDENT RESPONSE TEAM

The MGMT is responsible for incident detection and remediation of Information Resources. The MGMT will consult key representatives of F2OnSite's IT, Human Resources, Legal, Internal Audit, or other departments as warranted to establish an Incident Response Team appropriate to respond to a specific Incident.

As necessary, the MGMT and Incident Response Team shall assign Staff to manage specific security incidents:

- **Plan.** An Incident Response Plan (Plan) shall be developed. The Plan shall be reviewed and approved by the Executive Management or a committee that reports to Executive Management. The Plan shall document applicable state and federal laws, regulations, and standards to ensure response procedures meet appropriate requirements. The Plan shall identify third-party contact information that can assist with the incident and appropriate reporting. The Plan shall be tested at least annually to ensure it is sufficient and effective. The Plan shall be updated as a result of such tests.
- **Initial Investigations.** The Plan shall provide a quick and orderly response to incidents. The Plan shall identify steps to be followed for the initial reporting of events and subsequent investigations. Where appropriate, Staff shall be on call to handle incidents reported outside of standard business hours.
- **Risk Classification.** Initial investigations shall identify the incident severity level and classify the risk to the organization according to the guidelines contained in the Risk Assessment Classification section of this policy.
- **Documentation and Communications.** The initial investigations staff shall inform the MGMT of the Incident and the preliminary risk classification. The MGMT shall follow the guidelines identified in the Documentation and Communication of Incidents section of this policy.
- **Responder Procedures.** The MGMT shall identify the appropriate procedures and Staff to address the specific incident. Responders will attempt to identify as much information about the event so as to limit additional adverse effects. Responders

and appropriate Staff will evaluate and recommend to the MGMT appropriate actions to be taken.

- Special Situations/Exceptions. The MGMT shall identify and document procedures that address special situations and exceptions.
- Incident Reporting. The MGMT shall keep Executive Management informed on the status of current incidents. A post incident report shall be created.
- Training and Testing. The MGMT shall ensure Staff have the proper training to fulfill their incident response roles and responsibilities.

B. IDENTIFYING AND REPORTING INCIDENTS

The Incident Response Team shall work with F2OnSite departments to establish proactive monitoring systems that can identify potential incidents. Examples of incidents include, but are not limited to, ransomware, malware, data breach, Denial of Service (DoS), insider attacks, etc. In addition, any F2OnSite Staff may refer an activity or concern to IT Operations.

Once an incident has been reported, the Incident Response Team will log and track incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others, or otherwise address as outlined in the remainder of this policy.

In addition to reporting incidents, Staff shall report to the appropriate management any weaknesses or deficiencies in Information Resources.

C. RISK ASSESSMENT CLASSIFICATION

The MGMT will establish an internal risk assessment classification to focus the response to each incident, and to establish the appropriate team participants to respond. This classification matrix shall correspond to an “escalation” of contacts and indicate personnel at F2OnSite to be involved and procedures applicable for each class of incident.

In general, incidents are assigned to one of the following classifications:

- Unauthorized access – a person, process, or program is granted unauthorized physical or logical access to Information Resources. This classification includes a breach of sensitive data and should be reported to MGMT as soon as the incident is detected.
- Denial of service (DoS) – an attack that overloads an Information Resource to prevent it from performing its normal function. Distributed Denial of Service (DDoS) attacks are large-scale attacks from multiple sources.
- Malicious software (malware) – infects an operating system or application and prevents the software from performing its intended operation. In addition, the

malware may delete software and data, compromise the integrity of information, and disclose sensitive information to unauthorized personnel.

- Improper use – a person, process, or program that violates acceptable use policies. Examples include a disgruntled Staff member who ignores policies and procedures, a network administrator who circumvents log files, and a Staff member who extracts customer lists.
- Scans/probes/attempted access – an unauthorized person, process, or program that attempts to identify vulnerabilities through the use of vulnerability scanning, network mapping, and penetration testing tools.
- Other – this classification includes other types of incidents not described above. For example, unconfirmed incidents, potentially malicious events, or other activity that warrants additional review.

The MGMT, working with appropriate F2OnSite Staff, shall estimate the financial cost to respond to an incident for each of the above classifications. For example, the cost to respond to unauthorized access to personally identifiable or other Sensitive Information. Such information shall be conveyed to the F2OnSite Executive Management or a committee that reports to Executive Management.

D. DOCUMENTATION AND COMMUNICATION OF INCIDENTS

The MGMT shall ensure that incidents are appropriately logged and archived. Any incidents involving sensitive information shall be identified so the appropriate security procedures can be followed. The MGMT shall provide current status and reports to F2OnSite Executive Management.

Wherever possible, documentation of such incidents shall cross-reference other event databases such as IT ticket and network monitoring systems. Any incidents involving systems that are tracked in the inventory database shall be cross referenced in that database with the MGMT incident tracking log.

The MGMT or Incident Response Team representatives are responsible for communicating the incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the incident.

E. RESPONDER PROCEDURES

The MGMT shall maintain standard responder procedures for the response and investigation of each incident, as well as securing the custody of any evidence obtained in the investigation. The application of these procedures shall be governed by the classification described above as well as the Incident Response Plan. Staff shall refer to the Incident Response Plan for specific information on how to manage and respond to incidents. The procedures will specify the location, method of custody for each incident, and if custody of evidence is required.

F. SPECIAL SITUATIONS/EXCEPTIONS

Any personally owned devices, such as phones, wireless devices or other electronic transmitters which have been used to store sensitive information and are determined to contribute to an incident, may be subject to seizure and retention by F2OnSite Staff. By using personally owned devices within the F2OnSite network for business purposes, Staff are subject to F2OnSite policies restricting their use.

Proper forensic procedures, including chain of custody, shall be required for collection, retention, and presentation of evidence to support potential legal action. For more information about retention guidelines, see the Data Retention Policy.

Cloud computing controls shall be in place to ensure privacy and formal notification of a compromise of a Tenant's system(s).

G. INCIDENT REPORTING

The MGMT shall provide appropriate reporting to F2OnSite Executive Management. Such reporting to include, but is not limited to, updates to inform management of relevant details, risks, current status and progress, tasks to be completed, and expected outcomes and dates. Post incident reporting shall include appropriate details, mitigation actions, timeframes, and lessons learned.

In addition to reporting of specific incidents, the MGMT shall provide annual reporting to Executive Management that summarizing incidents reported and actions taken. The annual report shall identify numbers and types of incidents, impact, costs incurred, lessons learned, and other relevant factors.

Incident reports and supporting documents shall be retained in accordance with F2OnSite's Data Retention Policy.

On an on-going basis, the RMO shall identify data breach notification requirements. In the event of a data breach, the RMO shall notify F2OnSite Executive Management of relevant requirements so that appropriate action can be taken.

H. TRAINING

The MGMT shall be responsible for ensuring that incident response team members and related Staff have the proper training. Information shall be published for all Staff regarding the reporting of computer anomalies and incidents. Such information should be included in routine employee awareness activities.

Staff shall acknowledge their duties and responsibilities and agree to adhere to appropriate incident response policies, procedures, plans and related documents. No less than annually, awareness and refresher training shall be provided to maintain

incident response readiness and competency. The MGMT may also arrange incident response exercises to test and evaluate Staff, related procedures, and assess the ability to respond to incidents in a timely and effective manner.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Risk Management Officer, Chief Security Officer, Executive Management, Director of IT, and Security Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01
GDPR Article 33, 34
HIPAA 164.308(a)(6)(ii), 164.314(a)(2)(i), ARRA 13402
ISO 27001:2013 A.16
NIST SP 800-37 3.5, 3.7
NIST SP 800-53 AU-4, AU-6, AU-10(3), AU-11, CA-7, IR-4, IR-6, IR-8, SI-2, SI-4
NIST Cybersecurity Framework DE.AE-2-4, DE.CM-1-6, DE.DP-2, RS.MI-2, RC.RP-1
PCI 11.1.2, 11.5.3, 12.8.3, 12.10

INTERNET CONNECTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This policy has components of a user compliance policy and an internal IT policy. The user compliance section specifies how users are allowed to connect to the Internet and provides for IT Department approval of all connections to the Internet or other private network. It requires all connections such as connections by modems or wireless media to a private network or the Internet be approved by the IT Department and what is typically required for approval such as the operation of a firewall to protect the connection.

This policy requires users to use the Internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their Internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log Internet usage activity. Defines whether a proxy server will be used for user Internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

II. Purpose

This policy is designed to protect Information Resources against intrusion by malware that may be brought into the network by users as they use the Internet. It is also designed to prevent unauthorized and unprotected connections to the Internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

III. Scope

This policy applies to all Staff that have access to F2OnSite's Information Resources.

IV. Policy

All physical Internet connections or connections to other private networks shall be authorized and approved by the IT Department. Most users will access the Internet through the connection provided for their office by the IT Department. Any additional connections must be approved by the IT Department. These additional connections include but are not limited to:

- A computer or communication device which may allow a connection to the network.
- Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT Department.
- Wireless access points or devices with wireless capability are not allowed unless approved by the IT Department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT Department when connected to the network. Refer to the Wireless Access Policy for more information.
- Any additional Internet connections not provided by the IT Department must be reviewed and approved by the IT Department. Typically any additional connections from the organizational network to the Internet or other private network will require.
- An IT Department approved firewall operating at all times and properly configured. Refer to the Firewall Policy for more information.
- Some communications may require encryption. Contact the IT Department and/or refer to the Encryption Policy for more information.

An Internet control and logging system shall provide the following capabilities:

- The system will require a login ID or it will use the current network login to identify users.
- The system will prevent users from visiting inappropriate, pornographic, or dangerous web sites. This same system will not require an additional login ID and will use Active Directory to identify Internet users. The system shall be able to log the time of Internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.
- Refer to the Logging Policy for more information.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.04, APO13.04, BAI09.04, BAI10.10, DSS01.04, MEA01.04

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)

ISO 27001:2013 A5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

INTRUSION DETECTION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

II. Purpose

This policy establishes intrusion detection and security monitoring to protect resources and data on F2OnSite's network. It provides intrusion detection implementation guidelines along with associated roles and responsibilities.

III. Scope

This policy applies to all Staff that have access to F2OnSite's Information Resources.

IV. Policy

The objectives of this policy are to:

- Increase the level of security by actively searching for signs of unauthorized intrusion.
- Prevent or detect the confidentiality of organizational data on the network.
- Preserve the integrity of organizational data on the network.
- Prevent unauthorized use of organizational systems.
- Keep hosts and network resources available to authorized users.
- Increase security by detecting weaknesses in systems and network design early.

Intrusion detection provides two important functions in protecting Information Resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

All systems accessible from the Internet or by the public must operate IT approved active intrusion detection software during anytime the public may be able to access the system.

All systems in the DMZ must operate IT approved active intrusion detection software.

All host based and network based intrusion detection systems shall have their log files reviewed on a daily basis.

All intrusion detection logs must be kept for a minimum of 30 days. This provides an audit trail of past events. Operating system, user accounting, and application software audit logging processes are to be enabled on all host and server systems.

Alarm and alert functions of any firewalls and other network perimeter access control systems are to be enabled. Audit logging of any firewalls and other network perimeter access control system are to be enabled and audit logs from the perimeter access control systems will be monitored/reviewed daily by the Chief Security Officer (MGMT).

System integrity checks of the firewalls and other network perimeter access control systems will be performed on a routine basis. Audit logs for servers and hosts on the internal, protected, network will be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the MGMT.

Host based intrusion tools will be checked on a routine and all trouble reports should be reviewed for symptoms that might indicate intrusive activity.

Incident Response security controls must not be bypassed or disabled. All personnel are responsible for managing their use of incident response and are accountable for their actions relating to incident response security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.

All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments shall have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

All suspected and/or confided instances of successful and/or attempted intrusions will be immediately reported according to the Incident Response Plan. Users shall be trained to report any anomalies in system performance and signs of wrong doing to the Help Desk. Any suspected intrusions, suspicious activity, or system unexplained erratic behavior discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour.

The intrusion detection team shall:

- Monitor intrusion detection systems both host based and network based.
- Check intrusion detection logs daily.
- Determine approved intrusion detection systems and software.
- Report suspicious activity or suspected intrusions to the incident response team.

The incident response team shall:

- Act on reported incidents and take action to minimize damage, remove any hostile or unapproved software.
- Recommend changes to prevent future incidents.
- Action shall be based on the approved Incident Response Plan.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with information security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(C), 164.312(b), 164.312(e)(2)(i)

ISO 27001:2013 9.1, A.12.1.3, A.12.4

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AU-3, AU-6, AU-9, AU-11, AU-12, AU-14, RA-3, RA-5, SI-2, SI-5

NIST Cybersecurity Framework DE.AE-1-5, DE.CM-1-6, RS.RP-1, RS.MI-2

PCI 10.1-9

IT GOVERNANCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Information Technology (IT) governance is a part of the organization's corporate governance. IT governance is focused on Information Resources and their performance and risk management. IT governance helps ensure that the organization properly manages its IT projects, service delivery, and compliance requirements.

II. Purpose

IT governance is a process designed to manage the application of technology to business needs. IT governance qualifies initiatives as projects by ensuring alignment with the enterprise architecture and compliance requirements.

III. Scope

This policy applies to F2OnSite's Executive Management and the IT Director.

IV. Policy

The F2OnSite's IT governance and management framework exists to:

- Align the organization's IT with the organization's business goals and objectives
- Enable high-quality enterprise IT planning and management
- Define the roles and responsibilities necessary to create and sustain a comprehensive governance, planning and management framework
- Enable new strategic capabilities that allow F2OnSite to operate efficiently and effectively
- Identify and manage risk and protect F2OnSite's Information Resources

The IT Director provides the central point of accountability, leadership, vision and coordination for the enterprise. The IT Director is responsible for:

- Design - design and implement processes necessary to govern, plan, manage, oversee, evaluate and implement business planning, technical architecture, standards, information and telecommunications resource management planning, budgeting, funding, quality assurance, IT asset inventory and management, IT procurement, IT security, and IT performance standards and measurements
- Governance - provide governance for enterprise IT coordination, planning, decision-making, and policy development
- Tracking - coordinate, facilitate, track and report to executive management, the status of IT projects
- Communications - develop and implement IT communications and management support infrastructure including enterprise focused information sharing
- Policy - create the policies, standards and practices necessary to carry out the directives of F2OnSite management as they pertain to IT
- Initiatives - act as the sponsor for IT initiatives including research, identification and development of opportunities, proof-of-concept, etc.
- Assessment - establish and maintain a technical assessment capability through which to evaluate information and telecommunications technologies and management practices

Policies and procedures shall require management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Executive Management and the IT Director.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.01, EDM01.03, EDM02.03, EDM03.02, EDM03.07, APO01.03, MEA03.01
GDPR Article 24, 28, 37
HIPAA 64.308(a)(2), 164.308(b)(4), 164.314(a)(2)(i)
ISO 27001:2013 5, 9, A.5
NIST SP 800-37 3.1, 3.7
NIST SP 800-53 All XX-1 controls, PM-24, SI-5
NIST Cybersecurity Framework ID.GV-1-4, DE.CM-1-6, DE.DP-2
PCI A3.1.2, A3.2.2, A3.3.3

IT MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This companion policy to the Acceptable Use Policy sets forth department level responsibilities for the operation and maintenance of computers and networks.

II. Purpose

IT is critical to maintaining F2OnSite's business operations. This policy ensures sufficient resources are allocated to supporting and managing IT and its use within F2OnSite.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

The Chief Security Officer shall be responsible for the development and implementation of security policies and procedures. A formal job description shall identify the responsibilities of the Chief Security Officer and shall reflect the size of the organization, type of information collected, stored, processed, and transmitted, complexity, and technical capabilities of the organization.

Each operating department shall adopt policies governing the use of its IT resources using whatever procedures it normally follows for adopting policies in the department. Such policies shall be consistent with F2OnSite's Acceptable Use Policy and shall include at minimum the following components:

- A statement identifying the kinds of IT resources in the department and establishing general policies for each kind of resources. These policies should require the operating department to identify the persons responsible for each kind

of resource, the persons authorized to use the resources, and the uses permitted for the resources. Where appropriate, the policy should cover issues of shared access, resource limitations, and personal use.

- A policy statement regarding mission continuity planning to address system, application, and data backups and procedures for the recovery and restoration of department's mission critical IT resources in the event of loss.

If a department's IT usage does not warrant the development of department specific policies, the department may exercise the option of adopting F2OnSite's IT policies as its department level policies.

Departments that do not adopt department policies, and departments that do not have more restrictive policies on personal use of IT resources, shall be deemed to have adopted a policy prohibiting personal use by employees of telephones, pagers, cell phones, computers and other IT resources when such use interferes with the efficient performance of an employee's duties or with the functionality of the department's IT system or when it results in increased operating costs for the department or the F2OnSite. Subject to supervisor discretion, incidental personal use of IT resources that does not produce the above effects is authorized. Employees must promptly reimburse the department for any personal use of telephones, cell phones, or other IT resources that result in long distance toll charges or other identifiable increased costs for the department.

A. RESPONSIBILITY TO MAINTAIN FUNCTIONALITY

Each information system at F2OnSite is intended to serve some function or set of functions. The department's IT Coordinator shall ensure that the IT systems in the department continue to serve their functions with an appropriate degree of reliability.

The department's IT Coordinator shall facilitate appropriate training and IT knowledge transfer within the department. User training helps employees remain current or expand their technical skills and knowledge of applications. IT Coordinators should direct system users within their respective department to avail themselves of IT training support departments available both within and outside the F2OnSite. The department's IT Coordinator is also responsible for communicating important technical information to the users of the department's systems.

B. SECURITY RESPONSIBILITIES

The IT Director shall establish information security objectives. The objectives shall be consistent with F2OnSite's Security Policy, be measurable (if practical), take into account information security requirements and the results from a recent risk analysis, and be communicated to the appropriate staff.

When planning how to achieve information security objectives, the IT Director shall determine what needs to be done, resources required, responsible parties, timeframes, and how the results will be evaluated.

IT shall provide leadership and direction for the F2OnSite's network and systems security. IT has developed and implemented a network architecture that places an emphasis on security. F2OnSite's IT security team will develop system security awareness practices, appropriate system safeguards and effective responses to breaches in security within the departments. Security in a networked environment must be a responsibility shared by everyone. A single compromised workstation can be used to attack other systems both within and outside the F2OnSite.

IT Coordinators are responsible for establishing, communicating and enforcing department level practices and procedures that promote security. The following areas should be covered:

- Physical security.
- Protection of information, which includes periodic backup and offsite rotation of mission critical systems, applications, and data files.
- Prevention of unauthorized access.
- Detection of security breaches.
- Procedures for reporting security breaches to management or appropriate authority.
- Account auditing which includes the removal of accounts no longer authorized access to the F2OnSite's information technology resources. IT Coordinators and technical managers will work with IT security personnel, other system administrators, and law enforcement officials, both inside and outside the F2OnSite, to find and correct problems caused on any network or on another system by the use of the system under their control. Where violations of this or any other IT policy come to the IT Coordinator or Technical Manager's attention, they are authorized to take reasonable actions to maintain the security of the system. A user's access privileges may be temporarily suspended if the IT Coordinator or Technical Manager believes it is necessary or appropriate to maintain the integrity of the computer system or network.

The IT Director shall ensure:

- Appropriate contacts with relevant authorities are established and maintained.
- Appropriate contacts with relevant special interest groups (SIG) or specialized security forums and professional associations are established and maintained.
- Information security is addressed in project management regardless of the type of project.

C. RESPONSIBILITY TO PREVENT UNAUTHORIZED OR INAPPROPRIATE ACCESS AND DISCLOSURE

IT Coordinators are responsible for department level safeguards and procedures that minimize the possibilities of unauthorized access to F2OnSite or personal files. As matter of F2OnSite policy, no one, including IT Coordinators, Technical Managers and their staff members, may access user files except in the circumstances described below. Even where access is permitted, those who have accessed information must not reveal it to others who are not authorized to receive it. Technical Managers must configure their systems to minimize the possibilities for any unintended disclosure of personal information. In instances where a department does not have a Technical Manager, the IT Coordinator has the responsibility to arrange for the proper configuration of the department's systems.

D. PERMISSIBLE ACCESS BY IT COORDINATORS, TECHNICAL MANAGERS, AND STAFF

Investigation of System Problems - IT Coordinators, technical managers and their staff members are permitted to access user accounts, files or communications when there is reason to believe that the user is interfering with the performance of the system or network, but only to the extent reasonably necessary to ascertain whether there is a problem and to take corrective measures. In situations in which the IT Coordinator and the Technical Manager have no reason to suspect misconduct on the part of the user, the technical manager or staff member shall advise the user prior to access to the extent reasonably practicable. In situations in which misconduct is suspected, the technical manager or IT Coordinator shall first notify the appropriate authority for investigating disciplinary matters involving the particular user prior to attempting to gain access.

In no case shall a technical manager be restricted from immediately accessing any account, file or communication on a system for which the manager has responsibility, or from taking corrective action, where there is a reasonable belief that a failure to do so will result in loss of system or network stability, substantial damage to the system or network, or liability to the F2OnSite.

E. INVESTIGATION OF MISCONDUCT

As part of an investigation into possible violations of F2OnSite rules or policies, or of local state or Federal laws, individual user accounts, files and communications may be accessed as part of the investigation upon a showing that there is reason to believe that the accounts, files or communications contain information relevant to the infractions under investigation. With the exception of authorized IT security personnel, access to a suspect system will not be granted by the IT Coordinator or technical manager without appropriate approvals. In all cases, an authorized IT investigator shall notify the user prior to accessing the user's accounts, files or communications, except where reasonable efforts to contact the user are unsuccessful or upon a showing that prior notification would compromise the investigation. Pending approval of the appropriate

administrative head of a department, the authorized investigator may take reasonable steps to ensure that the accounts, files or communications are not altered or destroyed.

F. WHERE REQUIRED BY LAW

The F2OnSite will permit access to individual accounts, files and communications where required to comply with a lawfully issued subpoena, court order, Public Records Act request and other request having the force of law.

G. ACCESS FOR COWORKERS

Each operating department shall develop policies regarding shared access to F2OnSite files by coworkers and administrators. In situations in which a co-worker or administrator cannot access files for which they have authorization (because of the absence of an employee on whose workstation they are stored), an IT Coordinator or technical manager, with the approval of the department head, may make such files and only those specific files available to the authorized individual.

H. RESPONSIBILITY FOR POLICY ADHERENCE

The Office of the Vice President For Information Technology shall provide F2OnSite-wide leadership over department level adherence to the IT Management Policy. It is expected that departments and offices will become aligned to a department within six months of the F2OnSite's adoption of this policy.

Actual department-level policies should be developed and shared with the Office of the Vice President For Information Technology within one year of the F2OnSite's adoption of the IT Management Policy. Future newly formed departments will have one year to develop a department-level policy for submission to the Office of Information Technology.

IT will monitor department-level progress and will offer assistance to facilitate department formation, department-level policy development and overall compliance to the IT Management Policy. IT Coordinators and technical managers share the responsibility for seeing that F2OnSite and local policies governing the use of the system and network are followed. IT Coordinators and technical managers also have the obligation of ensuring that protections for the F2OnSite's user community are upheld.

Technical Managers may resolve minor or inadvertent violations. Where more serious violations of such policies have occurred or are suspected, it is the responsibility of the IT Coordinator to assist an investigation by an appropriate authority.

I. SYSTEM USER RESPONSIBILITIES

Consistent with the F2OnSite Acceptable Use Policy, this policy does not relieve ordinary users of personal computers or systems of the responsibility to maintain and

protect the integrity and security of information technology resources. If a computer is connected to the F2OnSite network, the user is responsible for ensuring that the computer is not used to compromise the security of the network. If the computer contains F2OnSite information resources, the user is responsible for data integrity, data backup, physical security of the machine, and for protecting the system from computer viruses and other attacks. In most departments, there are support personnel who will assist the user with these responsibilities.

J. MAINTENANCE OF INFORMATION SYSTEMS

Information Systems shall be properly maintained to sure system integrity, availability, and confidentiality. The IT Director shall ensure that:

- Maintenance activities are properly monitored and managed.
- Controls are implemented to restrict access to tools, techniques, mechanisms, and personnel used to conduct Information System maintenance.
- Data is securely removed from the Information System prior to taking the equipment off-site for maintenance.
- Media containing maintenance, diagnostic, or test programs is checked for malware before the media is used in the Information System.
- Multifactor authentication is employed to protect Information Systems when remote (non-local) sessions are used to maintain equipment. Maintenance sessions are to be terminated when the remote maintenance work is complete.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.01-03, APO01.05, APO01.07, APO01.11, APO13.07, BAI04.05, DSS04.05
GDPR Article 24, 28, 37
HIPAA 64.308(a)(2), 164.308(b)(4), 164.314(a)(2)(i)
ISO 27001:2013 5, 9, A.5
NIST SP 800-37 3.1, 3.7
NIST SP 800-53 All XX-1 controls, PM-24, SI-5
NIST Cybersecurity Framework ID.GV-1-4, DE.CM-1-6, DE.DP-2
PCI A3.1.2, A3.2.2, A3.3.3

LOGGING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This policy provides guidelines on the monitoring and logging of F2OnSite's Information Resources including F2OnSite's network and communications systems.

II. Purpose

This policy is established to protect the integrity, availability and confidentiality of information, to prevent loss of service, and to comply with legal requirements. This policy ensures that all Information Systems generate appropriate audit logs.

III. Scope

This policy applies to all F2OnSite IT system administrators, IT security Staff, the IT Director, and the Chief Security Officer.

IV. Policy

Without frequent monitoring and logging, it is difficult to assess the effectiveness of access controls. Unauthorized access can remain undetected, enabling information to be disclosed to persons with possible malicious or fraudulent intent.

Access to F2OnSite's network and communications shall be logged and monitored to identify potential misuse of systems or information. System access must be monitored regularly to prevent attempts at unauthorized access and to confirm that access control systems are effective.

Logs shall be kept secure and are only available to personnel authorized by IT Management. Such logs shall only be kept as long as necessary as outlined in F2OnSite's Electronic Data Retention Policy.

F2OnSite's information Systems shall be monitored and logged:

- Ensure use is authorized
- Manage and administer of systems
- Protect against unauthorized access

- Verify security procedures
- System and operational security
- Comply with F2OnSite's policies and procedures
- Detect and prevent crime
- Identify, report, and correct information and Information Systems flaws in a timely manner

A. Underlying requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit logging information:

- Determine the activity that was performed
- Who or what performed the activity, including where or on what system the activity was performed (subject)
- Systems involved (object)
- When the activity was performed
- Tools used
- The status (such as success vs. failure), outcome, or result of the activity

The IT Director shall ensure that local logging has been enabled on all systems and networking devices. The Chief Security Officer (MGMT) shall ensure that a centralized logging server has been implemented, configured, and all critical devices log to the server. The IT Director shall ensure important events and audit trials are logged for analysis and review. A file integrity monitoring/change detection software shall review logs and issue alerts if the log data is altered.

B. Activities to be logged

If audit trail reports and event logs are not regularly reviewed, incidents can remain undetected. IT staff shall be assigned to review and monitor the logs. Logs shall be reviewed on a regular and on-going basis. The frequency review shall be according to the sensitivity of the information stored and maintained. Procedures should verify that logging is active and working properly:

- Ensure events are properly classified
- Review logging for performance delays
- Ensure compliance related logging cannot be "turned off"
- Verify access to log files is properly restricted
- To assist with investigations, all critical system clocks and times should have their date and time synchronized using Network Time Protocol (NTP)
- Time data shall be protected and time settings shall be received from industry accepted time sources

System events shall be logged at the time activities are to be performed:

- System start up, restart, or shut down
- Application process startup, restart, or shutdown
- Read, write, update, or delete authentication information (e.g. IDs, passwords)
- Initiate or accept a network connection

- Grant, modify, or terminate access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system

Access to information shall be logged:

- Read, write, update, or delete Sensitive Information
- User authentication and authorization such as user login and logout
- Read, write, update, or delete information identified by the Chief Security Officer (MGMT) as needing to be logged

The MGMT shall implement automated audit trails for all Information Systems and components to reconstruct the following events:

- All individual user accesses to sensitive information
- All actions taken by any individual with root or administrative privileges
- Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system level objects

C. Elements of the log

System events and activities that should be monitored and logged include:

- System administrator and system operator activities
- System start-ups and shut-downs
- Logging start-ups and shut-downs
- Backups
- Exceptions
- Security events
- Protection software
- Protection hardware (firewalls, routers, etc.)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems
- Modifications to data characteristics including permissions, location, file type
- Authentication successes and failures (e.g. log in, log out, failed logins)

Application logging requires more than just relying on server logs. Application logs help identify security incidents, establish baselines, providing information about problems and unusual conditions, assist with incident investigation, and help detect attacks. Application events and activities that should be monitored and logged include:

- Application authentication (e.g. successes, failures, logouts)
- Data audit trails (e.g. access to sensitive data, adding data, modifying data, deleting data, exporting and importing data)
- Input validation failures (e.g. protocol violations, unacceptable encodings, invalid parameter names and values)
- Output validation failures (e.g. database record mismatch, invalid data encoding)
- Suspicious behavior (e.g. multiple records deleted in a short period of time, invalid access attempts)
- Session management failures (e.g. cookie session identification value modification)
- Application errors and events (e.g. syntax and runtime errors, connectivity problems, third party service error messages, file system errors, sequencing failure)
- Higher-risk functionality (e.g. network connections, adding and deleting users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of administrative privileges, access by application administrators, access to sensitive data, use of data encrypting keys, key changes, creating and deleting system-level objects, data import and export including screen-based reports, submission of user-generated content)
- Legal and other opt-ins (e.g. permissions to access credit history, terms of use, permission to receive marketing communications)
- Security events or warnings

Log entries and automated audit trails should include:

- Host name, system component, or resource
- Date
- Time
- Application ID (e.g. name and version)
- Initiating process or origination of event (e.g. entry point URL, page, form)
- Code location (e.g. module, subroutine)
- User initiating action (e.g. user ID)
- Event type
- Result status (e.g. success, failure, defer)
- Resource (e.g. identity or name of affected data, component)
- Location (e.g. IP address or location)
- Severity of event (e.g. emergency, alert, fatal error, warning, information only)
- Other (e.g. parameters, debug information, system error message)

D. Formatting and storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs should be collected by a centralized log management system

- Logs should be stored in a documented format and sent via reliable network protocols to a centralized log management system
- Logs stored in a SQL database that itself generates audit logs in compliance with the requirements of this Policy
- Other open logging mechanisms supporting the above requirements

E. Information Security Issues

Logs are one of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems. Detailed procedures that support this policy shall be developed to protect against log security risks such as:

- System administrators and those with operating system command line access can disable or circumvent access control and audit log mechanisms
- Staff with command line access can execute system commands that can damage and corrupt the system, data files, and/or log files
- The contents of system logs should be protected from unauthorized access, modification, and/or deletion; write once read many (WORM) drives may be an acceptable solution
- Emergency access to systems shall only be used in extreme circumstances and only when authorized by IT Management. Emergency access may by-pass traditional security controls and access to information resources or Company data shall be logged
- As a log approaches its maximum size, it can either overwrite old events or stop logging new events. This makes it susceptible to attacks in which an intruder can flood the log by generating a large number of new events. A partial defense against this is to increase the maximum log size so that a greater number of events is required to flood the log
- Administrators can change the auditing policies to stop logging an unauthorized activity. Log settings should be set to track and record log policy changes (audit policy change setting)
- Given the ability of administrators to manipulate log files to cover unauthorized activity, F2OnSite IT Management shall ensure a separation of duties between operations and security monitoring. Frequent backups of the log to a server accessible only to the security monitoring staff can improve security
- Keeping the IT department's security systems and practices confidential helps prevent users from formulating ways to cover their tracks. If users are aware that the log is copied over to the remote log server at :00 of every hour, for instance, they may take measures to defeat that system by attacking at :10 and then deleting the relevant log events before the top of the next hour]
- If an Administrator account has been compromised, the event history, as contained in the log, is unreliable; a WORM drive or remote log server with all services disabled (allowing only console access) might be acceptable solutions

The MGMT shall be responsible for:

- Ensuring a regular review of activity audit logs, access reports, and security incidents. Approving the types of logs and reports to be generated, review activities to be performed, and procedures that describe the specifics of the reviews
- Procedures that specify monitoring log-in attempts, reporting discrepancies, and processes used to monitor log-in attempts
- Procedures that specify audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.

Procedures ensure that the audit controls meet security requirements by recording and examining activity related to sensitive information

- Securing audit trails by limiting viewing of audit trails to those with a job-related need, protecting audit trail files from unauthorized modifications, ensuring audit trail files are promptly backed up to a centralized log server or media that is difficult to alter, writing logs for external facing technologies onto a log server on the internal log server or media device, and using file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (new data being added should not cause an alert)
- Software activity involving critical assets and sensitive data is tracked. Attacks are detected and the impacts and effects of attacks are minimized

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all IT system administrators, IT security Staff, the IT Director, and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM02.03, APO11.09, APO12.02, APO13.07, BAI04.05, BAI09.04, DSS01.05, DSS05.02
 GDPR Article 25, 32
 HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(b), 164.312(b)
 ISO 27001:2013 9.1, 9.3, A.12.1.3, A.12.4
 NIST SP 800-37 3.3, 3.7
 NIST SP 800-53 3.4, AC-2, AC-8, AC-17, AU-6, AU-13, CA-7, CM-1
 NIST Cybersecurity Framework PR.DS-4, DE.AE-1-4, DE.CM-1-6, DE.DP-2, RS.RP-1
 PCI 6.3, 10.1-9, A1.3, A3.2.2.1, A3.3.1, PCI Software Security Framework

LOGICAL ACCESS CONTROLS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This policy controls logical, electronic access to information systems and applications.

II. Purpose

The purpose of this policy is to define logical access controls as they relate to F2OnSite Information Resources. Logical access controls are tools used for identification, authentication, authorization, and accountability in Information Resources. Logical access controls can be embedded within operating systems, applications, add-on security packages, or database and telecommunication management systems.

III. Scope

This policy applies to the Information Resources data owners and security staff that implement controls to govern access to Information Resources.

IV. Policy

Without Logical access controls shall be established and documented for all F2OnSite Information Resources. The access controls shall be implemented based upon the principle of least privilege.

A Risk Assessment shall be performed for the purpose of identifying Information Resources and sensitive data. A Risk Treatment Plan shall be prepared and updated annually that defines safeguards and controls to protect such Information Resources.

All access to Information Resources shall use an approved method of identification and authentication per the Identification and Authentication Policy. All third party service provider access to the F2OnSite network and information systems must adhere to the same access restrictions as internal users.

Access rights shall be established, documented, and periodically reviewed based on business needs and external requirements. Access controls should consider:

- Security requirements given business needs, anticipated threats, and vulnerabilities.

- Relevant legislative and regulatory requirements.
- Contractual obligations and service level agreements.
- Consistency across F2OnSite's systems and networks.

Access control considerations include:

- The use of clearly stated rules and rights based on user profiles.
- Consistent management of access rights across Information Resources using an appropriate mix of logical (technical) and physical access controls.
- Segregation of access control roles including access request by the appropriate department, access authorization by the Data Owner, and access administration by the Network Administrator.
- Requirements for the formal authorization and timely removal of access rights.

All critical Information Resources must limit and enforce access to only the times identified as necessary for completion of F2OnSite business processes. All access to these systems and applications at all other times shall be disabled or suspended.

All access to any database containing Sensitive Information (including access by applications, administrators, and all other users) shall be restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Sessions that are inactive must be automatically terminated. The amount of time permitted before session termination must be aligned with the criticality of the information. Approved compensating controls, e.g. password protected screensavers or terminal locks, must be activated for information systems and applications that cannot automatically terminate sessions.

All critical information systems and applications must not allow users to have multiple concurrent sessions on the same system.

All information systems must have, or support, password management systems that are interactive and can ensure strong passwords to meet the requirements of the Security Policy.

All information systems must not transmit passwords in clear text and passwords must not be visibly displayed on the system when being entered.

Users given the opportunity to login to information systems must be presented with a login banner that includes a special notice informing the user that the system is to be used only by authorized users and that the use of the system constitutes consent to monitoring.

All Information Systems, databases, and applications that store authentication information such as a user ID and password must be encrypted with access restricted to only authorized personnel.

Utilities that are capable of overriding information system and application controls or performing low-level system maintenance must be approved with additional controls implemented to restrict their use.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Information Resource security Staff, System Administrators, Data Owners, and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B)

ISO 27001 A.6.2.2, 7.2.1, A.8.1.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC-1, PR.AC-3-4, PR.AC-7, DE.DP-2, RS.RP-1

PCI 7.1-3

MASS COMMUNICATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite is committed to protecting its Information Resources, Staff, customers, partners and its operations from illegal or damaging actions by individuals, either knowingly or unknowingly. F2OnSite assets are to be used for business purposes in serving the interests of the company and of our clients and customers in the course of normal operations.

II. Purpose

The purpose of this policy is to ensure F2OnSite's ability to communicate and deliver messages consistently, in both emergency and nonemergency situations, in a manner that is both appropriate and effective and that best serves the organization's strategic missions, goals, reputation and image.

III. Scope

This policy covers all mass communications to all staff and business contacts via hard copy and across all media, required to operate the F2OnSite.

IV. Policy

F2OnSite uses five types of mass communication messages:

1. Crisis and/or emergency, including unscheduled F2OnSite closings
2. Changes to policies and/or changes or interruptions to standard operating procedures
3. Official communications
4. Official solicitations
5. General information

Mass communications are those print or electronic messages which are directed to audiences that exceed a Vice President's area of responsibility and are sent without self-subscription or opt-out capabilities. In most cases, electronic communication is preferable to paper communications.

All internal mass communications shall be limited to official business or official activities of F2OnSite. Employee e-mail addresses will be used as the primary channel of communication for all mass

communication messages. In those areas where employees do not have access to electronic means of communication, it is the responsibility of the Department Head to identify a system for communicating messages to these employees. Examples of internal mass communication messages include:

- Unscheduled F2OnSite closings due to environmental (e.g. weather) or terrorist activities
- Change in personnel related issues (e.g. holidays, health care benefits, working hours)
- Security reminders

Emergency announcements shall temporarily be placed on the Staff portion of the F2OnSite intranet. In addition, automated messages can be sent to Staff voice mail.

External mass communications shall be limited to official business or official activities of F2OnSite. Examples of external mass communications include:

- Press releases
- Marketing product and service announcements
- Customer communications

The F2OnSite President or appropriate designate shall review and approve all mass communication messages before they are distributed internally, externally, or both.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO05.03, APO10.05, APO12.02, BAI02.05, BAI04.05, MEA01.05

GDPR Article 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.310(a)(2)(i)

ISO 27001:2013 7.4, 8.1

NIST SP 800-37 3.1, 3.7

NIST SP 800-53 IR-1, IR-4, PM-31

NIST Cybersecurity Framework ID.AM-2, ID.GV-4, PR.AC-1, PR.AC-4, PR.AC-7, PR.DS-1-5

PCI 12.10

MERGERS AND ACQUISITIONS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's strategic plan includes the ability to grow market share and revenues by merging or acquiring other entities. When merging or integrating Information Resources it is important that F2OnSite Staff understand and agree on the appropriate procedures to protect F2OnSite's assets.

II. Purpose

The purpose of this policy is to establish responsibilities related to mergers and acquisitions (M&A) of outside entities and their Information Resources. This policy also defines minimum security requirements related to integrating outside systems with F2OnSite's Information Systems.

III. Scope

This policy applies to all F2OnSite Staff (current as well as merged/acquired) that have access to F2OnSite's Information Resources.

IV. Policy

A. M&A Assessment Team

Merger and Acquisition (M&A) assessments are performed to ensure that the new entity's Information Resources do not pose a risk to F2OnSite.

F2OnSite will assemble an assessment team consisting of members of the following departments:

- Chief Security Officer
- Legal Department
- IT security

The purpose of the M&A assessment team is to identify and analyze risks related to Information Resources, develop a risk treatment plan, and implement risk reduction and corrective action prior to integrating the new entity's systems with F2OnSite's Information Resources.

B. Security Requirements

The following minimum requirements must be achieved before the new entity's systems can be integrated with or connected to F2OnSite's Information Resources:

- Data Center – must comply with F2OnSite's Physical Security Policy
- Facilities – must comply with F2OnSite's Physical Access Policy
- Firewalls – must comply with F2OnSite's Firewall Policy.
- Laptops and other mobile devices – must comply with F2OnSite's Portable Computing Policy
- Routers – must comply with F2OnSite's Router Security Policy
- Security Protection – must comply with F2OnSite's Anti-malware Policy
- Servers – must comply with F2OnSite's Server Hardening Policy.
- Wireless – must comply with F2OnSite's Wireless Access Policy.
- Workstations – must comply with F2OnSite's Workstation Security Policy.

Staff from the new entity must receive appropriate training commensurate with their job duties. At a minimum, users must comply with F2OnSite's administrative related policies including, but not limited to:

- Acceptable Use Policy
- E-mail Policy
- Password Policy
- Remote Access Policy
- Removable Media Policy
- Reporting Violations Policy

C. M&A Assessment Report

Once the risk reduction and risk treatment strategies have been implemented, the assessment team will deliver an M&A Assessment Report to F2OnSite Legal Department. The M&A Assessment Report will document:

- Initial status of new entity's systems
- Actions taken to reduce or transfer risks
- Residual risks that remain after risk reduction strategies
- Written recommendation related to the risks

The Legal Department will review the M&A Assessment Report and make a recommendation to F2OnSite Executive Management to either proceed with the integration, accepting any residual risk, or delay the integration until such time as the new entity's systems can meet the above requirements.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01-05, APO02.08, APO08.05-06, APO09.05, APO10.05, APO12.02, APO12.07
 GDPR Article 25, 29, 32
 HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(2)
 ISO 27001:2013 8.1-3, 9.3, A.5.1.2, A.6.1.1-2, A.7.3, A.9.2.6, A.12.1.2, A.14.2.2
 NIST SP 800-37 3.1, 3.4, 3.5
 NIST SP 800-53 CM-3, CM-5, CM-9, CP-2, PS-7, SA-3, SA-9-10, SI-2, PM-2, PM-10, PS-4-5
 NIST Cybersecurity Framework ID.AM-3, ID.BE-4, ID.GV-3, ID.RA-1, ID.SC-1, PR.AC-1
 PCI 12.2, A3.1.2, A3.2.3

MOBILE DEVICE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Mobile computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

II. Purpose

The purpose of this Policy is to establish the rules for the use of Mobile devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of information.

III. Scope

This policy applies to all F2OnSite Staff that utilize portable (mobile) computing devices and access F2OnSite Information Resources. All mobile devices, whether owned by F2OnSite or owned by Staff, that have access to Information Resources are governed by this Mobile Device Policy. Applications, including cloud storage software, used by Staff on their own personal devices are also subject to this policy.

IV. Policy

Only IT Department approved mobile computing devices may be used to access F2OnSite networks and Information Resources.

All mobile computing devices must be protected with a password required at the time the device is powered on. The password must meet the requirements of F2OnSite's Password Policy.

Sensitive data shall not be stored on mobile computing devices. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques per the Encryption Policy.

Data must not be transmitted via wireless to or from a Mobile Device unless approved wireless transmission protocols along with approved encryption techniques are utilized. See the Wireless Access Policy for more information.

Non-F2OnSite mobile computer devices that require network connectivity must conform to F2OnSite IT standards and must be approved in writing by the IT Department.

Unattended mobile computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Laptops and other mobile computing devices that access F2OnSite's Network Infrastructure shall have active and up-to-date anti-malware and firewall protection. Personal firewalls shall be installed and activated on mobile and/or employee owned devices that connect to the Internet when outside F2OnSite's network and which are also used to access F2OnSite's network.

Annual security education and awareness training shall be provided to Staff that use mobile devices. Such training shall include:

- Minimum necessary. Staff shall only have access to the minimum amount of data necessary to perform their job duties.
- Lost devices. Staff must immediately report any lost or stolen devices.
- Unauthorized access. Any unauthorized access to the mobile device or company data must be immediately reported.
- Rooting devices. Mobile devices must not be "rooted"* or have unauthorized software/firmware installed.
- Content. Staff shall not load illegal content or pirated software onto a mobile device.
- Software installs. Only approved applications are allowed on mobile devices that connect to F2OnSite's network and data.
- Patch management. Mobile devices and applications must be kept up-to-date. Patches should be installed within 30 days of release.
- Anti-malware. Mobile devices must have active and up-to-date anti-malware protection software.
- Encryption. Encryption shall be used to protect sensitive information.
- Firewalls. Where possible, personal firewalls shall be installed and active (i.e. not disabled).
- Work habits. Staff shall use F2OnSite's corporate e-mail system when sending or receiving company data.
- Backups. Staff are responsible for ensuring all important files stored on the mobile device are backed up on a regular basis.
- Management software. Mobile device management software will be used to enforce common security standards and configurations.

The Chief Security Officer (MGMT) shall ensure:

- Firewalls. Specific configuration settings are defined for personal firewall software. Controls are established to ensure that personal firewall software is not alterable by users of mobile and/or employee-owned devices.
- Training. Annual security training is provided to users of mobile devices. Periodic security reminders may be used to reinforce mobile device security procedures.

- Mobile device management. An evaluation is performed to determine the appropriate Mobile Device Management software to be used to reduce costs and business risks related to mobile devices. Features of Mobile Device Management software include the ability to inventory devices, monitor devices (e.g. application installations), issue alerts (e.g. disabled passwords, out of date operating systems, rooted devices), and issue reports (e.g. installed applications, carriers). The MGMT shall ensure Mobile Device Management software enforces security features such as encryption, password, and key lock on mobile devices. The MGMT shall perform a review to determine if Mobile Device Management software should include the ability to distribute applications, data, and configuration settings.
- Security. The MGMT shall remain up-to-date on industry standard security best practices for mobile devices. Resources can include NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST Special Publication 800-124).
- Exemptions. A risk assessment and risk analysis shall be performed for any requests for exemptions from this Policy.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from mobile computing devices which are generally higher-risk than non-portable devices (e.g., desktop computers).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO10.05, APO12.02, APO13.07, BAI02.05, BAI03.05, DSS01.05, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001:2013 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-1, ID.GV-4, ID.RA-4, PR.AC-1-4, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2

NETWORK ADDRESS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

The IT Department is responsible for planning, developing, implementing and maintaining F2OnSite's network. The use of Internet Protocol (IP) and network addresses is included in this responsibility.

II. Purpose

Internet Protocol and network addresses are numeric labels assigned to each network device. The address serves two principal functions, to identify a host or network interface and to identify a location. The purpose of this policy is to ensure network addresses are properly assigned and managed.

III. Scope

This policy applies to IT Department Staff responsible for managing F2OnSite networks.

IV. Policy

The IT Department Network Administrators are assigned the responsibility of managing F2OnSite's IP and network addresses.

Addresses may be assigned to a device either at the time of startup (dynamic), or permanently assigned (static) by a fixed configuration of its hardware or software. The IT Department shall maintain procedures for implementing, maintaining, and terminating IP and network addresses.

Where possible, Network Administrators shall centrally manage the addresses without having to specifically configure each device on the network as a manual procedure. Dynamic IP addresses can be configured on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. This avoids the administrative burden of assigning specific static addresses to each device on a network. It also

allows many devices to share limited address space on a network if only some devices are connected at a particular time. Dynamic IP configuration shall be enabled by default so that a user does not need to manually enter settings to connect to a network with a DHCP server.

Systems requiring access to the Internet shall be configured with public (global) IPv4 or IPv6 addresses.

IP or network addresses that are not in use for a period of three months shall be brought to the attention of the Director of IT for resolution.

Network administrators may elect to implement host access controls based on network address. Network addresses may be grouped into subnets of a reasonable size taking into account the types of devices, uses, quantities, physical layout of the network, and ease of network management.

Network Administrators may allocate network addresses within a particular subnet or VLAN. VLANs are generally allocated with one subnet per VLAN for all devices connected to the network. Network Administrators shall maintain a register of VLAN names and address ranges.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the IT Department Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO03.06, APO12.02, APO12.07, APO13.07, DSS06.08, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5.1.1, A.8.1.1, A.8.2.2
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 CM-8, SC-2, SC-7, SC-21
NIST Cybersecurity Framework ID.AM-5, ID.BE-4, ID.RA-6, ID.SC-1, PR.PT-4, DE.DP-2
PCI 1.3.7

NETWORK CONFIGURATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite Information Systems are provided as a resource for all F2OnSite Staff that have access to F2OnSite's network, internal systems, and Internet services. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in networking technology.

II. Purpose

The purpose of this policy is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of F2OnSite information.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

F2OnSite's IT Department is responsible for managing F2OnSite's network infrastructure and related equipment including firewalls, routers, switches, cabling, servers, etc. The IT Department will manage maintenance and enhancements to this infrastructure.

To provide a consistent F2OnSite network infrastructure capable of exploiting new networking developments, all cabling must be installed by the F2OnSite IT Department or an approved contractor.

All network connected equipment must be configured to a specification approved by the F2OnSite IT Department. In addition, all hardware connected to the F2OnSite network is subject to F2OnSite IT Department management and monitoring standards.

Changes to the configuration of active network management devices must not be made without the approval of F2OnSite IT Department.

The F2OnSite network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the F2OnSite IT Department. The networking addresses for the supported protocols are allocated, registered and managed centrally by F2OnSite's IT Department.

All connections of the network infrastructure to external third party networks is the responsibility of F2OnSite's IT Department. This includes connections to external telephone networks.

The IT Department must adhere to F2OnSite's Firewall Policy when installing and configuring software or hardware firewalls. The use of departmental firewalls is not permitted without the written authorization from F2OnSite's IT Department.

Firewalls, routers, and switches shall be securely configured. Configuration and security standards for network infrastructure devices including firewalls, routers, switches, virtual environment, servers, workstations, and related components shall be developed and maintained.

Network environments shall be designed and configured to restrict connections between trusted and untrusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure. Sub networks shall be implemented and maintained for public accessible components that are physically or logically separated by internal networks.

Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts. Physical and logical access to diagnostic and configuration ports shall be controlled.

An external and accurate time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate the tracing and reconstitution of activity timelines. Specific legal jurisdictions and orbital storage and relay platforms (US GPS & EU Galileo Satellite Network) may mandate a reference clock that differs in synchronization with the F2OnSite's domicile time reference. In this case, the jurisdiction or platform is treated as an explicitly defined security domain.

Configuration management ensures that protection features are implemented and maintained in the system. Configuration management shall be used to apply a level of discipline and control to the processes of system maintenance and modification.

- Configuration Documentation. Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security relevant software product names and version or release numbers, and physical location.
- System Connectivity. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.
- Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure shall be documented.

The configuration program shall be documented in a configuration management plan and shall include:

- Formal change control procedures to ensure the review and approval of security relevant hardware and software.
- Procedures for management of all documentation, such as the system security plan and security test plans, used to ensure system security.
- Workable processes to implement, periodically test, and verify the configuration management plan.
- A verification process to provide additional assurance that the configuration management process is working effectively and that changes outside the configuration management process are technically or procedurally not permitted.
- Procedures that monitor growth and traffic patterns to ensure traffic loads can be handled without interruption.

When connecting two or more networks:

- IT security Staff shall review the security attributes of each network (even if the networks are certified at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.
- The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires certification as a unit.

Systems that process information at different classification levels or require different formal access approvals can be interconnected if:

- Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or
- Both systems are accredited to process the level of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

Any information system connected to another system that does not meet the above requirements shall utilize a Controlled Interface that performs the following:

- A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.
- A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.
- Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the communication interface shall notify the user of the communication and forward the communication only on request from the user). If Sensitive Information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

Controlled Interfaces shall filter information in a data stream based on associated security labels for data content:

- There shall be no general users on the Controlled Interface.
- There shall be no user code running on the Controlled Interface.
- The Controlled Interface shall provide a protected conduit for the transfer of user data.

- Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

Controlled Interfaces shall have the following properties:

- Differences. The Controlled Interface shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.
- Routing Decisions. The Controlled Interface shall base its routing decisions on information that is supplied or alterable only by the security support structure.
- Restrictive Protection Requirements. The Controlled Interface shall support the protection requirements of the most restrictive of the attached networks or IS.
- User Code. The Controlled Interface shall not run any user code.
- Fail-secure. The Controlled Interface shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.
- Communication Limits. The Controlled Interface shall ensure that communication policies and connections that are not explicitly permitted are prohibited.
- In general, such systems have only privileged users; i.e., system administrators and maintainers. The Controlled Interface may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The Controlled Interface application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the Controlled Interface if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

Each Controlled Interface shall be tested and evaluated to ensure that the Controlled Interface, as implemented, can provide the separation required for the system's protection level.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO03.06, APO12.02, APO12.07, APO13.07, DSS06.08, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2)
ISO 27001:2013 A.8.1.3, .A9.1, A.9.4.1, A.12.1.2
NIST SP 800-37 3.2, 3.4
NIST SP 800-53 3.5, CM-1, CM-3-4, CM-6-7, SA-5
NIST Cybersecurity Framework ID.AM-1-6, ID.BE-4, ID.RA-5, ID.RM-1, DE.CM-1, DE.DP-2
PCI 1.1, A2.1

NETWORK DOCUMENTATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Networks are critical to the business operations of F2OnSite. Network documentation helps F2OnSite adhere to industry best practices, reduces downtime and makes the troubleshooting process more efficient when problems arise.

II. Purpose

This policy details the aspects of the network that need to be documented, especially each server. This policy also communicates to each system administrator exactly what is expected regarding the documentation process.

III. Scope

This policy applies to system administrators at F2OnSite. This policy applies whether the equipment is owned or leased by F2OnSite.

IV. Policy

The network structure and configuration shall be documented with a map of the network's topology including:

- Each network segment
- Gateways
- Routers
- Firewalls
- Servers

While the information included in a network topology diagram is not necessarily specific, there is certain information that must be included for each server, even if that information has to be placed in an appendix. For each server, documentation shall include the server's name, its IP address and the role that the server is performing (DNS, DHCP, mail server, etc.). Documentation shall describe situations where the servers have multiple IP addresses or network interface cards.

An Information Systems Log Form shall be maintained as a part of the network documentation. This form shall detail changes such as patch and application installations, modified security settings, system maintenance, backups, and errors.

Software applications, versions, and manufacturer contact information shall be provided as a part of the network documentation. Documentation shall include software applications and their versions running on each server. Copies of the software licenses shall be retained in hardcopy or electronic format.

Documentation shall include network components such as switches, routers, gateways and other networking hardware. As appropriate, the documentation shall include:

- How the device is connected to the network
- How the device is configured
- Configuration backups
- Firmware revision
- Document Active Directory
- Domain names in the forest
- Active Directory site structure
- Where servers exist within the Active Directory hierarchy
- The location and contents of each group policy
- Any external trusts that may exist

The backup methodology shall be documented and include backup software used, version, backup media, rotation schedule, off-site storage, where media is stored, etc. See the Backup Policy and Backup Plan for more information.

Network Infrastructure and related system documentation shall be protected against unauthorized access but shall be made available to those who need it to perform their duties.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite IT Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02-03, APO05.05, APO11.09-10, APO12.02, APO12.07, APO13.07, BAI11.09

GDPR Article 25

HIPAA 164.316(b)(1)

ISO 27001:2013 5.2, 6.1.2, 6.2, 7.2, 7.5, 8.1, 9.1

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 CM-8, PM-5, RA-1, SA-5

NIST Cybersecurity Framework ID.RA-1, ID.RA-3, PR.PT-1, RS.MI-3

PCI 1.1, 1.5, 2.4-5, 3.5 -7, 4.3, 5.4

NETWORK SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Networks are a growing and important asset for F2OnSite (Company). They provide a critical competitive advantage in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our Staff use networks to connect with our customers, service providers, and other key organizations, it is important that Staff understand and agree on the appropriate procedures to protect F2OnSite's assets.

II. Purpose

This policy outlines the principles, procedures, and guidelines to identify, manage, and maintain security on F2OnSite's computer network. It is designed to ensure that our computer network and data is protected from security breaches.

III. Scope

This policy applies to the Chief Security Officer, department heads, and all Staff that implement and maintain Information Systems.

IV. Policy

A. Classification

All F2OnSite network equipment (e.g. routers, servers, workstations) shall be classified and placed in a network segment appropriate to its level of classification. Access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification, the data shall be protected in a manner appropriate to its classification level.

All users, hosts, and data shall be classified as security level 1 Public (information intended or required for public release), security level 2 Sensitive (sensitive data that requires additional levels of protection), or security level 3 Confidential (sensitive data that must be protected from unauthorized disclosure or public release). See the Data Classification Policy for more information. All physical network segments, IP subnets and other IP traffic carriers must be classified in the same way. All data travelling on a network

must be classified, and all users using network equipment or requesting data over the network must be assigned a level of clearance according to the same system.

It is the function of the person designated as the Resource Owner to have all equipment under his or her control classified. Classification shall be performed in consultation between the Resource Owner, or an assigned representative, and the Chief Security Officer (MGMT), but the final decision shall lie with the MGMT.

Classification of Users

Every user shall be designated as unclassified until the user's classification is explicitly changed with the written approval of the MGMT. When new Staff join F2OnSite, a request may be made by the appropriate manager to the MGMT for a new level of clearance. It is the responsibility of the manager to justify the requested level of clearance.

Unless there is strong justification, all new Staff shall be cleared for the level F2OnSite Only, but only after they have signed acceptance F2OnSite policies and non-disclosure forms.

The MGMT is responsible for managing and controlling the record of clearance levels for all personnel. It is the responsibility of all Resource Owners and system administrators to determine the security level of a given user before granting that user access to any system.

It is the responsibility of the user to know his or her clearance level and to understand the rights and limitations associated with that clearance.

Classification of Networks

The MGMT shall classify network segments that constitute part of the F2OnSite infrastructure. A complete list of the classifications of all network segments in the F2OnSite network and in the F2OnSite backbone shall be maintained by the MGMT. Classifications for existing F2OnSite network segments are as follows:

- Public – F2OnSite's backbone, remote sites, server local area network, portal segment.
- Sensitive – user local area networks.
- Confidential – Server local area network, backup server local area network.

Classification of Equipment

The MGMT shall assign a classification to all equipment. The MGMT shall be responsible for maintaining a complete list of the classifications of all Information Systems in the F2OnSite network. Classifications for F2OnSite equipment are as follows:

- Public – backbone equipment (e.g. switches, remote access servers) that is not located on premises. Equipment used in the transfer of data to and from the Internet.
- Sensitive – user workstations, print servers, etc.
- Confidential – servers and other hosts used in the management of the F2OnSite's backbone infrastructure and network infrastructure.

Classification of Data

For more information see the Data Classification Policy.

B. Network Segmentation

Network segmentation shall be implemented to limit the impact of a network intrusion. Historically, a firewall was implemented at the boundary of an organization's trusted internal network to the untrusted Internet. Creating one trusted internal network zone wasn't sufficient as it created an environment that allowed an attacker to breach one component and gain widespread access to internal systems. Segmenting a network into smaller groups enhanced security and reduced the impact of an intrusion.

Unless otherwise stated in this Policy, all network segments shall be classified Level 1 - Unclassified. A network segment can only be classified as another security level with approval of the MGMT. Applicable Resource Owners shall be notified of changes in classifications.

Network equipment shall not be connected to a network segment that is not of the same security level as the equipment itself. The MGMT may choose to segment two networks of the same security level.

C. Trusted Points

Wherever a network segment connects to another network segment with a different security level, the connection between the two networks shall be controlled by an approved trusted point. A trusted point shall include equipment capable of ensuring the security of traffic between two network segments in a manner appropriate to the classification of the networks.

Trusted points shall be under the control of the MGMT. Access to any trusted point shall only be granted with the explicit permission of the MGMT. The trusted point used to segment two networks shall be appropriate for the network with the higher security level. The MGMT shall determine approved connections and related controls between network segments.

Connections into Public segments from

- Public – no controls
- Sensitive – no controls
- Confidential – no controls

Connections into Sensitive segments from

- Public – via a proxy with network level control to and from the proxy, strong user level control
- Sensitive – no controls
- Confidential – no controls

Connections into Confidential segments from

- Public – not permitted
- Sensitive – strong user level controls
- Confidential – no controls

Examples of trusted point technologies include:

- Network level controls – Transmission Control Protocol (TCP) wrappers, allow lists on hosts, router filters, network level firewalls, virtual local area network (V-LAN) switches etc.
- User level controls – application proxies and user level firewalls.

- Strong user level controls – token-based user authentication systems, certificates. Whenever there is a connection that skips over a security level, strong user level control must be used. Even if strong user control is used, a connection may never skip more than one security level.

D. Security Controls

The MGMT shall ensure sufficient and effective security controls are implemented and maintained to protect F2OnSite's internal network.

Access – Information Resources shall be protected against unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication, and implementing access controls on Information Resources. Inactivity timeouts and screen savers shall be used to protect against unauthorized access to systems. Accounts shall be locked after a number of failed logon attempts. For more information see the Identification and Authentication Policy and Securing Information Systems Policy.

Anti-virus – desktop and laptop computers must have anti-virus software or filters installed and updated. In addition, workstations and servers must have anti-virus software installed and updated daily. For more information see the Anti-Malware Policy.

Authentication – access to Sensitive Information shall be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator level passwords shall be exceptionally strong. Wherever possible, user accounts with fewer privileges shall be used instead of administrator accounts. Periodic review of access shall be performed. Password management systems shall be interactive and shall ensure quality passwords. For more information see the Password Policy.

Backups – periodic backup copies of software, data, and system configurations shall be made, tested, and stored in a secure manner. The physical security of the removable media shall be maintained and plans made to allow recovery from unexpected problems. For more information see the Backup Policy.

Communications – processes deny network communications traffic by default (i.e. deny all) and only allow network communications traffic by exception. Communications over unauthorized TCP or UDP ports or application traffic shall be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries. Security mechanisms prevent remote devices from simultaneously establishing non-remote connections with the Information System while also communicating via some other connection to external networks. Communications with known malicious or unused Internet IP addresses shall be denied and access limited only to trusted and necessary IP address ranges at each of the organization's network boundaries.

Configuration – Information Systems shall be configured in accordance with applicable F2OnSite security guidelines and standards. When received from a vendor, computers and other devices may not be configured for security and may require initial as well as ongoing review of the configuration and security of the operating system and software. For more information see the Configuration Management Policy and Network Security Policy.

Design – Information System design and software development principles shall promote effective information security. Processes shall be implemented to monitor, control, and protect Information Systems from information transmitted or received at the external boundaries and key internal boundaries of the Information Systems. An inventory of all of the organization's network boundaries shall be implemented and maintained.

Disposal – a secure deletion program shall be used to erase data from hard disks and media prior to transfer or disposal of hardware. Permanent media (e.g., CD's, etc.) must be physically destroyed. For more information see the Disposal Policy.

Documentation – network documentation shall be kept up-to-date and be available to authorized personnel. The documentation shall be reviewed annually by a Documentation Analyst to verify it is appropriate, sufficient, and effective at continuing Information Resource availability, confidentiality, and integrity. For more information see the Documentation Policy.

Encryption – cryptographic controls prevent unauthorized disclosure of data during transmission unless otherwise protected by alternative physical safeguards. Authentication data (e.g. user ID and password) and the data itself must use strong encryption. Encryption of Sensitive Information stored on Mobile Computing Devices is required. Encryption is sufficient and effective and according to the classification of the data. Keys are properly managed and maintained. For more information see the Encryption Policy.

Firewall – a software firewall, hardware firewall, or other network filtering technology shall be used to limit network access to the device storing Sensitive Information. For more information see the Firewall Policy.

Incident detection – security policies and procedures identify processes that monitor and analyze security alerts and information, establish, document, and distribute security incident response and escalation procedures, and ensure timely and effective handling of all situations. For more information see the Security Monitoring Policy and Incident Response Policy.

Information Systems – devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures. These reviews must include adherence to baseline security requirements as well as additional strategies for protecting the information. Devices shall be managed using multi-factor authentication and encrypted sessions. For workstations see the Workstation Security Policy. For servers, see the Server Hardening Policy.

Intrusion Detection – Network based Intrusion Detection Systems (IDS) shall be deployed at each of the network's boundaries. IDS sensors shall examine activity to identify unusual attack mechanisms and detect compromise of these systems.

Logging – Information System log files shall be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in the event of a security incident. Logs shall be of sufficient capacity to store at least 90 days of activity. For more information see the Logging Policy.

Owner – Information Systems shall have an identified Resource Owner, such as the principal user of the data or a department supervisor responsible for the data and can act as a point of contact.

Patching – security vulnerabilities are identified on a regular basis. Information Systems shall be patched and updated on a regular and recurring basis. Automatic settings or centralized updating of security patches is recommended for most workstations. For more information see the Patch Management Policy and System Update Policy.

Physical Access – physical access to Information Systems shall be restricted as much as possible. Where applicable, devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops shall be physically restrained (e.g. via an anchoring device) and servers must be in an appropriate and secure physical facility. Risks related to copying, moving, and storing of sensitive information on removable electronic media shall be managed. Information Systems are not to be taken off-site without prior approval from the Data Owner. For more information see the Securing Information Systems Policy, Physical Access Policy, and Physical Security Policy.

Segmentation – networks shall be segmented to protect Information Systems and Sensitive Information. Network segment shall be based upon the classification level of the information stored on the servers. Sensitive Information shall be stored on separate Virtual Local Area Networks (VLANs).

Sensitive Information – one or more of the following shall be used to protect Sensitive Information:

- Maintain an inventory of all Sensitive Information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider
- Ensure Sensitive Information is stored on hardened servers/devices
- Restrict the volume and duration of Sensitive Information
- Store Sensitive Information on dedicated systems with no other applications or data
- Restrict access to internal systems or devices that contain Sensitive Information
- Encrypt Sensitive Information both in transit and when stored including mobile devices
- Vendor notifications of security updates/patches are implemented in a timely manner
- Automated tools on network perimeters shall monitor for unauthorized transfer of Sensitive Information and blocks such transfers while alerting IT security Staff
- Remove from the network sensitive data or systems not regularly accessed. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.

Services – Web servers, ftp servers, mail servers, peer-to-peer networks, and anonymous file sharing software can significantly increase the risk to Sensitive Information. As much as possible, services on Information Systems or other devices shall be limited. Unless a high level of expertise is available, and these services shall be closely monitored at all times, higher risk software should not be installed. The IT Department shall be responsible for the installation and maintenance of software. For more information see the Hardware and Software Maintenance Policy.

Third Party Service Providers – risks related to service providers shall be managed and include controls such as remote access is only activated when needed, service provider actions are monitored, and access is immediately terminated when the provider has completed their service. In addition, agreements with service providers shall include appropriate wording related to confidentiality, data breaches, security controls, and audits. For more information see the Third Party Service Providers Policy.

E. Data in Transit

Network technologies are regarded as either "safe" or "unsafe" in their native state (i.e. without any encryption). Data transmitted between any two network-components is considered to be "data in transit". Data in transit also includes all control and management sessions.

All data in transit over an unsafe network segment that has a classification lower than the classification of the data must be protected by strong data encryption. Data in transit over a safe network segment may be encrypted.

Encryption of data in transit may include:

- Network encryption – data is encrypted at the Internet Protocol (IP) layer (e.g. IPsec)
- Session encryption – data is encrypted at a TCP layer (e.g. TLS)
- Message encryption – blocks of data are encrypted before they are sent (e.g. SMIME)
- Data encryption – the entire data package is encrypted before it is transmitted (e.g. file encryption)

For more information see the Encryption Policy.

F. Responsibilities

The MGMT shall:

- Approve and maintain a list of all classifications
- Approve F2OnSite's network design and topography
- Control and manage all trusted points
- Ensure security controls are implemented and maintained

Resource Owners and system administrators shall:

- Determine the security level of a given user before granting that user access to any system
- Verify the classification of the equipment they manage
- Verify that the equipment is installed and protected in accordance with its classification

Department heads shall:

- Obtain clearance for Staff in the department
- Clarify the classification of data on systems under the control of the department head
- Clarify the classification of Information Systems under the control of the department head

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Chief Security Officer, department heads, and all Staff that implement and maintain Information Systems.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5, A.7.2.2, A8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

OUTSOURCING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite uses outsourcing as a means of reducing costs, accessing specialist expertise, and providing greater focus on non-core functions. This process must be managed to ensure the proper benefits are received and risks remain within acceptable levels.

II. Purpose

Outsourcing involves the use of third party service providers to perform activities on a continuing basis (including agreements for a limited period), that would normally be undertaken by F2OnSite. This policy manages the risks related to outsourcing.

III. Scope

This policy applies to all Staff responsible for outsourcing F2OnSite functions and activities.

IV. Policy

Department Heads shall ensure that outsourcing arrangements do not diminish F2OnSite's ability to meet our contractual and compliance obligations. Procedures shall be identified to ensure that the outsource provider employs the same standard of care in performing the services as would be employed by F2OnSite. Department Heads shall not engage in outsourcing activities that have a high likelihood of damaging F2OnSite's image and reputation.

Per the Risk Assessment Policy, The Risk Assessment and Risk Treatment Plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks. During the annual review, Department Heads shall review risks and controls related to outsourcing. Material outsourcing arrangements have the potential to significantly impact F2OnSite's business operations, reputation, and profitability. Department Heads shall use the following indicators to determine outsourcing materiality:

- The level of importance of the service provided by the outsourcer
- The potential impact on our organization should the outsourcer be unable to provide services
- The potential impact of an outsourcer security breach
- Outsourcer costs and related cost controls

Outsourcing risks that should be evaluated and analyzed by the Department Heads include:

- Strategic Risk – the outsourcer may conduct business in a manner inconsistent with that of F2OnSite
- Image Risk – unsatisfactory performance may impact F2OnSite's image and reputation
- Operational Risk – the server provider may experience a failure in business operations and be unable to meet its contractual service levels or performance obligations
- Compliance Risk – F2OnSite may face compliance related risks related to privacy, security, and regulatory issues
- Legal Risk – F2OnSite may be faced with fines or penalties
- Termination Risk – the loss of in-house Staff with specific skill sets might make it more difficult to terminate an agreement with an outsourcer

Outsourcing to any third party service provider can create risks that must be managed, regardless of the location of the provider. Outsourcing to cross-border jurisdictions presents additional risks that must be managed:

- Issues related to distance and/or different time zones
- Risks related to the actions of foreign governments
- Relying on a foreign legal system for enforcement

When analyzing an outsourcing arrangement, Department Heads should consider:

- The ability of the service provider to comply with its obligations and meet the performance service levels required by the department
- The compatibility of F2OnSite's Information Resources with those of the service provider
- Excessive outsourcing arrangements with the service provider
- Outsourcer staff is subjected to background checks equivalent to those performed on F2OnSite's Staff

The outsourcing of any activity does not diminish our obligations and those of Executive Management who have the ultimate responsibility for the outsourced activity. Outsourcing a business process or function shall not interfere with the ability of a department to effectively oversee and manage its activities.

F2OnSite is responsible for the actions of the outsourcer and the confidentiality of information collected, transmitted, stored, or processed by the third party service provider. Department Heads shall consider compliance, contractual, and legal requirements when qualifying, evaluating, and selecting an outsourcer. Department Heads shall comply with F2OnSite's Third Party Service Providers Policy.

Department Heads shall:

- Communicate material outsourcing risks to Executive Management in a timely manner
- Ensure procedures are in place to continuously monitor service provider performance to ensure services meet pre-established requirements
- Ensure that outsourcing contingency plans are in place and tested at least annually
- Ensure an independent review and audit of the outsourcer to ensure that risks remain within acceptable levels.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Department Heads.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO06.09, APO07.12-13, APO09.05, APO10.05, APO11.09-10, MEA01.05
GDPR Article 25, 26, 28, 32
HIPAA 164.308(a)(1)(ii)(A), 164.308(b)(4), 164.502(b)(1), ARRA 13404(b), ARRA 13405(b)
ISO 27001:2013 8.1, A.13.1.2, A.14.2.7
NIST SP 800-37 3.3, 3.7
NIST SP 800-53 PS-7, RA-9, SA-4, SA-10-12, SA-15, SA-17
NIST Cybersecurity Framework ID.AM-4-6, ID.BE-4, ID.GV-2, ID.RA-4, ID.RM-1, ID.SC-3-4
PCI 12.8

PASSWORD POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Computer accounts are used to grant access to ABC Company's Information Systems. The process of creating, controlling, and monitoring computer accounts is extremely important to an overall security program.

II. Purpose

Identification and authentication access controls play an important role in helping to protect Information Systems. The purpose of this policy is to protect Information Systems by defining requirements for new passwords and changes to passwords.

III. Scope

This policy applies to all ABC Company Staff that utilize Information Systems with IDs and passwords (credentials). This policy applies whether Staff is using ABC Company Information Systems, Staff owned devices for Company approved work, or Staff use Information Systems of third party service providers for work related activities.

IV. Policy

The Chief Security Officer (MGMT) shall ensure:

- Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases

- Policies and procedures prevent staff from sharing passwords/phrases with others.

- Procedures advise staff to commit their passwords/phrases to memory and not allow them to be written down.

- Policies and procedures govern the password/phrase change frequency.

- Policies and procedures dictate when passwords/phrases must be supplemented with additional access controls such as tokens and biometric.

This Policy applies to all ABC Company related authentication activities including, but not limited to, the following:

- Administrator accounts.
- User accounts.
- Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.).
- Third party service providers.
- Web applications.
- Screen savers.
- Mobile devices.

A. New User Accounts

When granting access for a new user/account:

- System administrators will establish a unique ID and unique password/phrase.
- The user password will be conveyed to the user in a secure manner.
- When the user logs on for the first time, the user will be required to change their initial password/phrase to something that meets the requirements of this policy.

B. Selecting Passwords/Phrases

The Chief Security Officer, working with the appropriate Data Owners, will determine the appropriate authentication methods to be used. In general, there are two options:

- Passwords change frequently. In this approach, passwords change every 90 days and users are not allowed to re-use the most recent 5 prior passwords. The advantage is that if someone becomes aware of a person's password, they only have a short time (90 days) to use it. The disadvantage is that users may have a large number of passwords that expire on a frequent basis.
- Phrases are not required to be changed on a regular basis. Users are educated to choose phrases (memorized secrets) that are long and complex. Phrases are not the same as passwords. A phrase is a longer version of a password and is typically composed of multiple words. The phrase "We're off to see the wizard, The Wonderful Wizard of Oz" can be converted to WotstwTWWoO. By converting some letters to numbers and special characters the phrase is even more secure. With this option, systems and applications need to allow phrases up to 64 positions in length. Due to the possible length of the phrase, the Staff member shall have the option of seeing the phrase as it is entered, not just a series of asterisks or bullets.

Where possible, a password/phrase strength meter shall be used to help ensure Staff select long, strong, and complex passwords/phrases that meet the following requirements:

Contain both upper and lower case characters (e.g., a-z, A-Z).

Include both numbers (0-9) and special characters (e.g. @, #, \$, *).

Have a minimum of at least 10 characters.

Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data.

Staff should not choose passwords/phrases that:

Include common words such as those found in a dictionary.

Are the same as passwords/phrases used on Staff personal accounts (e.g. personal e-mail, on-line banking, or social media).

Contain personal information such as a spouse or pet's name, social security number, driver's license number, street address, phone number, etc.

Contain sequences or repeated characters. For example, 1234, 3333, abcdef, etc.

Contain the name of the entity, application, or service.

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

C. Password/Phrase Guidelines

Staff shall follow security guidelines to ensure passwords/phrases are not compromised. Security training and awareness programs shall ensure Staff is:

- Educated on security related risks.
- Reminded of security requirements when selecting and protecting passwords/phrases.
- Educated not to select the "Remember Me" or "Remember Password" feature in web applications and browsers.
- Reminded to be careful when using social media so the password/phrase is not compromised.

Passwords/phrases must not be:

- Revealed to anyone.
- Stored, written down, or transmitted in clear (unencrypted) text.
- Inserted into unencrypted e-mail messages or other forms of electronic communications.

If a Staff member believes that their password/phrase has been compromised or made available to others, the Staff member must immediately change their password/phrase and notify IT security Staff.

If someone demands a password/phrase, refer them to this policy or have them contact the IT Department.

D. Password Changes

Passwords must be changed on a regular basis according to the following schedule:

All administrator passwords must be changed at least every 30 days.

All user passwords must be changed at least every 90 days.

When selecting a new password/phrase, Staff shall not repeat any of their prior five passwords/phrases.

E. Software Applications

Application developers must ensure programs contain the following security precautions:

- Applications must require each user to have their own unique ID (e.g. not shared, no user groups).
- Passwords/phrases and Sensitive Information must be protected using strong encryption.
- Passwords/phrases and Sensitive Information must not be transmitted or stored in clear text.
- Ensure applications timeout and require the user to enter a password/phrase after a period of inactivity.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO01.11, APO12.02, APO13.07, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(3)(ii)(A)

ISO 27001:2013 A9.3, A9.4

NIST SP 800-37 2.3

NIST SP 800-53 3.7, IA-2, IA-5

NIST Cybersecurity Framework PR.AC-1, PR.AC-3-4, PR.AC-7, DE.DP-2, RS.RP-1

PCI 2.1

PATCH MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This policy identifies the need to apply vendor-issued critical security updates and patches regularly to protect F2OnSite data and systems. It applies to all electronic devices connected to the network including servers, workstations, firewalls, network switches and routers, mobile devices, Smartphones, etc.

II. Purpose

Software is critical to the delivery of services to F2OnSite's customers, Staff, and business partners. This policy protects F2OnSite's assets and helps ensure our ability to continue business operations.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. The latest stable version of any security related updates shall be installed on all network devices. System components and devices attached to the Pacific Steel & Recycling network must be regularly maintained including the application of critical security patches within 30 days after release by the vendor. Other patches not designated as critical by the vendor must be applied on a normal maintenance schedule, which may depart from the above. Note: Critical security patches should be identified according to a risk ranking process.

After testing software patches and updates, automated software update tools shall be used, where possible, to ensure that operating system and third-party software applications are running the most recent security updates provided by the vendor. Many vendors have automated the patching procedure, particularly for desktop computers. While there is some potential for error by the vendor, the risks are substantially less than if patches are never applied at all due to oversight.

Patches on production systems (e.g. servers) may require complex testing and installation procedures. In certain cases, risk mitigation, rather than patching, may be preferable. The risk mitigation alternative

selected should be in proportion to the risk. The reason for any departure from the above standard and alternative protection measures taken must be documented in writing for devices storing non-public data.

The regular application of critical security patches is reviewed as part of the normal F2OnSite audit procedures.

Policies and procedures shall be established and mechanism implemented for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.

Patching should include updates to operating systems as well as office productivity software, data base software, third party applications (e.g. Flash, pdf, etc.), and mobile devices with access to F2OnSite Information Resources.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite IT Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.310(c)

ISO 27001:2013 A.11.2.4, A.11.2.6, A.12.1.2, A.12.6

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 RA-3, RA-5, SI-2, SI-5

NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2

PCI 6.1, 6.2

PCI Policy

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite values its relationships with our customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

II. Purpose

The Payment Card Industry Data Security Standard is a proprietary information security standard for organizations that handle cardholder information. A strong compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

III. Scope

This policy applies to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store customer payment card data.

IV. Policy

The Payment Card Industry Data Security Standard (PCI DSS) was developed to increase controls around cardholder data. Its purpose is to reduce credit card fraud that occurs as a result of unauthorized disclosure. As outlined in the following table, PCI DSS specifies 12 requirements for compliance, organized into six logically related groups (control objectives).

Control Objectives and PCI DSS Requirements
Build and Maintain a Secure Network and Systems 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program 5. Protect all systems against malware and regularly update anti-virus software or programs

6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures
7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
Maintain an Information Security Policy
12. Maintain a policy that addresses information security for all personnel

The IT Department shall document the flow of cardholder information. Such documentation shall consider the flow of information within F2OnSite as well as with external third party service providers.

The IT Department shall identify all sources and uses of cardholder data and prepare network and data flow diagrams that identify where cardholder data is collected, transmitted, stored, processed, and archived. The IT Department shall include, but not be limited to, software applications, network infrastructure equipment (e.g. servers, storage), backup/recovery sites, fail-over systems, and other relevant devices. IT Department documentation shall identify how the cardholder data environment was determined.

The Chief Security Officer (MGMT) shall ensure:

- The cardholder data environment identifies and documents the existence of all cardholder data and that no cardholder data exists outside of the defined environment. If cardholder data is found outside of the defined environment, the cardholder data should be securely deleted, migrated into the defined environment, or the defined environment should be expanded to include the additional cardholder data.
- Network segmentation is considered as a means of protecting the cardholder data environment. Network segmentation can be achieved through physical or logical controls that isolate and protect the cardholder data environment.
- Third party service providers validate compliance requirements by either having an assessment on their own providing sufficient evidence to customers or by participating in customer reviews of the service provider environment.
- Monitoring systems ensure security controls are operating effectively and as intended. Such controls include, but are not limited to, firewalls, intrusion detection and prevention systems (IDS/IPS), file integrity monitoring, anti-malware, and access controls. Failures in security controls shall be detected and responded to in a timely manner. Processes to respond to security control failures shall include restoring the security control, identifying the cause of failure, identifying and addressing any security issues that arose during the failure of the security control, implementing mitigating controls prevent the failure, and resuming monitoring of the security control.
- The cardholder data environment is periodically reviewed for changes and potential impact.
- Security controls are reviewed and updated as a result of changes in the organization or cardholder data environment.
- Periodic reviews are performed to confirm compliance with PCI requirements. Such reviews shall ensure that security controls are sufficient and effective at protecting the cardholder data environment. Documentation shall be retained as evidence of the reviews.

- Annual reviews of hardware and software are performed to confirm the environment is supported by the appropriate vendors and the environment meets applicable security requirements.
- Where possible, security and audit functions are separated from IT operations.
- Effective methods of data discovery are used to identify unencrypted cardholder data. Ensure response procedures are initiated upon the detection of unencrypted cardholder data.
- Data Loss Prevention (DLP) mechanisms detect and prevent unencrypted cardholder data from leaving the environment.

In addition to the above responsibilities, the MGMT shall ensure:

- Configuration rule sets are reviewed by System Administrators at least every six (6) months.
- The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
- Verification codes or values (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions are not stored.
- Personal identification number (PIN) or the encrypted PIN block are not stored.
- Primary Account Number (PAN) is masked when displayed. The first six and last four digits are the maximum number of digits to be displayed.
- PAN is unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One way hashes based on strong cryptography (hash must be of the entire PAN), Truncation (hashing cannot be used to replace the truncated segment of PAN, Index tokens and pads (pads must be securely stored), and strong cryptography with associated key management processes and procedures.
- Additional controls are in place when hashed and truncated versions of the same PAN are present in an environment.
- Only personnel with a legitimate business need can see the full Primary Account Number.
- Unprotected PANs are never sent by end-user messaging technologies (e.g. e-mail, instant messaging, chat, etc.).
- Devices that capture payment card data via direct physical interaction with the card are protected from tampering and substitution. Note: These requirements apply to card reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.
- An up-to-date list of devices is maintained. The list shall include make, model of device, location of device (e.g. address of the site or facility where the device is located), and device serial number or other method of unique identification
- Device surfaces shall be periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.
- Training is provided so personnel can be made aware of attempted tampering or replacement of devices. Training should include verification of the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices, Staff should not install, replace, or return devices without verification, Staff should be

aware of suspicious behavior around devices (e.g. attempts by unknown persons to unplug or open devices), Staff should report suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g. to their manager or the MGMT).

- Quarterly external vulnerability scans are performed via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
- Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission.
- Cardholder data storage is kept to a minimum, a Data Retention Policy and Disposal Policy exists, data storage and retention times are limited to that which is required for business, legal, and/or regulatory purposes, as documented in the Data Retention Policy.

The following data elements from the magnetic stripe, when properly secured, may be retained for business operations: Cardholder's name, Primary Account Number, Expiration date, and service code.

The IT Department shall develop and maintain an inventory of all systems that store, process, and/or transmit cardholder data. At a minimum, the following information shall be maintained:

- Name – name of the system or device
- Data – cardholder data stored including field names
- Description – include reason for collecting, storing, use, or transmitting information
- Retention – time period that cardholder data is retained per F2OnSite's Data Retention Policy
- Security – protection measures including encrypting, masking, hashing, truncating data

The IT Department shall implement safeguards and controls to meet PCI Control Objectives and PCI DSS Requirements. Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission. If wireless networks collect, store, process, and/or transmit cardholder data, the IT Department shall implement safeguards to protect the information. Such safeguards shall include:

- Defaults – change default passwords, service set identification (SSID) name
- Encryption – enable strong encryption (WPA or WPA2)
- Physical access – restrict physical access to wireless access points
- Logs – review and archive wireless log files per the Logging Policy and Data Retention Policy
- Usage – ensure use of wireless networks complies with Wireless Access Policy requirements

To meet PCI Software Security Framework – Secure Software Requirements, the MGMT shall ensure the following controls are implemented:

- The attack surface is minimized. Software critical assets are identified and classified. Default privileges, features, and functionality are restricted to only those necessary to provide a secure default configuration. Retention of sensitive data is minimized.
- Software protection mechanisms are implemented to protect the integrity and confidentiality of critical assets. Critical assets are protected from attack scenarios. Software implements strong authentication and access control to help protect the confidentiality and integrity of critical assets. Sensitive data is protected at rest and in transit. Cryptography is used appropriately and correctly.
- The software vendor facilitates secure software operation. Software activity involving critical assets is tracked. Attacks are detected and the impacts/effects of attacks are minimized.

- The Software Vendor implements secure software lifecycle management practices. The software vendor identifies, assesses, and manages threats and vulnerabilities to its payment software. The software vendor facilitates secure software releases and updates. The software vendor provides clear and thorough guidance on the secure implementation, configuration, and operation of the software.

To meet PCI Software Security Framework – Secure Software Lifecycle Requirements, the MGMT shall ensure the following controls are implemented:

- A formal software security governance program establishes responsibility and authority for the security of the vendor's products and services. The vendor allocates resources to execute the strategy and ensure that personnel are appropriately skilled. The vendor defines, maintains, and communicates a software security policy and a strategy for ensuring the secure design, development, and management of its products and services. Performance against the software security strategy is monitored and tracked.
- The vendor continuously identifies, assesses, and manages risk to its payment software and services. The vendor detects and mitigates vulnerabilities in the software and its components to ensure that payment software remains resistant to attacks throughout its entire lifetime.
- Identify and manage payment software changes throughout the software lifecycle. Protect the integrity of the payment software throughout the software lifecycle. The confidentiality of customer's sensitive production data on vendor systems is maintained.
- The vendor provides clear and thorough guidance on the secure implementation, configuration, and operation of its payment software applications. The vendor maintains communication channels with stakeholders regarding potential security issues and mitigation options. The vendor provides stakeholders with detailed explanations of all software changes.

F2OnSite policies and plans shall implement and maintain specific Safeguards to meet PCI compliance requirements.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff who have access to or manage Information Resources that collect, transmit, process, or store cardholder related data.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.07, MEA02.11, MEA03.01

GDPR Article 25, 32

HIPAA 164.312(a)(2)(iv), 164.312(c)(2)

ISO 27001:2013 A.9

NIST SP 800-37 3.1

NIST SP 800-53 IA-5

NIST Cybersecurity Framework ID.RA-6, PR.AC-1, DE.CM-1, RS.RP-1, RS.MI-2

PCI 1.1-5, 2.2-4, 2.6, 3.1-7, 4.1-3, 5.1-4, 6.1-6.2, 6.5, 6.6-7, 7.1-3, 8.1-8, 9.1-7, 9.9-10, 10.1-7, 10.8-9, 11.1-5, 11.6, 12.1-3, 12.5, 12.4-7, 12.8-11, A1, A2.1-3, A3.1-3, A3.2.1-6, A3.3.2, PCI Software Security Framework

PERSONNEL SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Each F2OnSite asset must be protected during its lifecycle from its creation through its disposal. Each asset must be classified and protected based on its importance to the organization.

II. Purpose

This policy defines requirements for the protection of corporate assets from abuse, misuse, or destruction. Each authorized user has an obligation to preserve and protect assets in a consistent and reliable manner. Security controls provide the necessary technical, physical, and operational safeguards to protect assets.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Asset protection plays an important role in ensuring information confidentiality, availability, and integrity. Protection measures are introduced at the recruitment or vendor procurement phase, included in the employee handbook and vendor contracts, and monitored during an individual's employment or use of third party service providers.

All Staff must protect both tangible and intangible corporate assets. Staff are responsible for reporting to the appropriate manager any real or suspected threats to corporate assets.

Information security responsibilities are to be followed by all Staff who have access to F2OnSite's Information Resources. All Staff must acknowledge in writing that they have read the appropriate Confidentiality Agreement.

Specific information security responsibilities must be incorporated into all contracts with Staff who have access to F2OnSite assets.

Information security training shall be provided by the IT Department on a regular basis to make Staff aware of information security policies, procedures, and responsibilities. All Staff shall be trained in the security requirements and processes associated with their job duties, services provided, appropriate business controls, and the correct use of IT systems and facilities.

All Staff must acknowledge in writing that they have read and understood F2OnSite's Security Policy. In addition, all Staff shall receive annual security related training.

Prior to hire, all employees must pass a background check that includes examination of criminal conviction records, credit bureau records, and verification of previous employment. On-going annual background checks shall be performed on all staff that have access to sensitive information.

All Staff must be trained to recognize conflicts of interest and the appearance of conflicts of interest during their first week of employment and annually thereafter. All Staff must identify and submit to their immediate supervisor any conflicts of interest. All conflict of interest statements must be reviewed by the Chief Security Officer (MGMT). If the MGMT identifies a significant conflict of interest, the conflicts must be discussed with the Staff member's immediate supervisor to determine the appropriate course of action.

All Staff must sign an F2OnSite Non-disclosure Agreement prior to beginning work for F2OnSite.

The MGMT will implement a system for security incident reporting, response, tracking, and resolution. All Staff are responsible for reporting to the appropriate F2OnSite manager any violations of this Policy.

The Human Resources Department is responsible for ensuring that background checks are performed on F2OnSite employees. The MGMT is responsible for implementing and maintaining Staff security education and awareness training programs. Refer to the Security Awareness and Training Policy for more information.

Executive management shall ensure that internal audit mechanisms exist to monitor and measure compliance with this policy. Department Heads are responsible for enforcing compliance with this policy.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO07.12-13, APO08.05-06, APO09.05, APO10.05, APO12.02, APO13.07, MEA01.05
GDPR Article 25, 32
HIPAA 164.308(a)(1)(i), 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i)
ISO 27001:2013 8.1, A.6.2.2, A.7.1, A.9
NIST SP 800-37 3.4, 3.6, 3.7
NIST SP 800-53 AC-1-3, AC-17, PE-17, PL-4, PS-6, PS-7, SA-9
NIST Cybersecurity Framework ID.AM-6, ID.RA-6, PR.AC-1-4, PR.AC-6-7, PR.AT-1, DE.DP-2
PCI 7.1-3, 8.1-2, 8.4-5, 8.8

PHYSICAL ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Technical support staff, system administrators, and security personnel are responsible for facility access requirements. The granting, controlling, and monitoring of physical access facilities is extremely important to an overall security program.

II. Purpose

The purpose of this policy is to establish the rules for the granting, control, monitoring, and removal of physical access to F2OnSite facilities.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Physical access to all restricted facilities must be documented and managed. All facilities must be physically protected in proportion to the criticality or importance of their function.

Requests for access must come from the applicable data/system owner. Access to facilities must be granted only to support personnel, and contractors, whose job responsibilities require access to that facility. The process for granting card and/or key access to facilities must include the approval of the person responsible for the facility. The person responsible for the facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access. Access rights to facilities shall be based on the individual's (i.e. Staff, visitor, contractor, etc.) role or function including control of access to software programs for testing and revision.

The Chief Security Officer (MGMT) shall ensure:

- Secure areas are protected by appropriate entry controls that ensure only authorized personnel are allowed access.
- Procedures control and validate a staff member's access to facilities with the use of guards, ID badges, key cards, etc.

- Procedures identify visitor controls such as visitor sign-in, wearing of visitor badges, escorting by authorized personnel, etc.
- Procedures for working in secure areas are designed and applied.
- Policies specify management's review of the list of individuals with physical access to facilities containing sensitive information.
- A complete inventory of critical assets shall be maintained with ownership defined and documented.
- Card access records and visitor logs for facilities are kept for routine review based upon the criticality of the information being protected.

Access cards and/or keys must not be shared or loaned to others. Cards/keys must not be loaned or given to another individual. Cards/keys must not have identifying information other than a return mail address. Cards/keys that are no longer required must be returned to the person responsible for the facility. Lost or stolen cards/or keys must be reported to the person responsible for the facility. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned. The person responsible for the facility must remove the card and/or key access rights of individuals that change roles or are separated from their relationship with F2OnSite.

The person responsible for the facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

Procedures shall be developed to identify and authorize visitors:

- All facilities that allow access to visitors will track visitor access with a sign in/out log.
- A visitor log shall be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where sensitive information is stored or transmitted. The visitor log shall document the visitor's name, the firm represented, and the on-site personnel authorizing physical access on the log. The visitor log shall be retained for a minimum of three months, unless otherwise restricted by law.
- Visitors shall be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from on-site personnel. Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration.
- Visitors shall be authorized before entering, and escorted at all times within, areas where sensitive information is processed or maintained. Visitors must be escorted in card access controlled areas of facilities.

Procedures shall be developed to easily distinguish between on-site personnel and visitors. Such controls to include, but not be limited to:

- Identifying new on-site personnel or visitors (e.g. assigning badges).
- Changes to access requirements.
- Revoking or terminating on-site personnel and expired visitor identification (e.g. ID badges).

Access to areas containing sensitive information must be physically restricted. All individuals in these areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible.

Access to restricted IT areas such as data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT resources shall be restricted based upon business need.

Physical access to records containing confidential or protected data, and storage of such records and data in locked facilities, storage areas or containers shall be restricted.

Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information.

Appropriate facility entry controls shall limit and monitor physical access to Information Systems. Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas. This excludes public-facing areas where only point-of sale terminals are present, such as cashier areas. Such data shall be stored for at least three months, unless otherwise restricted by law.

IT security Staff shall:

- Implement physical and/or logical controls to restrict access to publicly accessible data jacks. For example, data jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks. Areas accessible to visitors should not have data jacks enabled unless network access is specifically authorized.
- Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines.
- Control physical and logical access to diagnostic and configuration ports.
- Receive authorization prior to relocation or transfer of hardware, software or data to an offsite premises.

Physical access for on-site personnel to sensitive areas shall be controlled:

- Access must be authorized and based on individual job function.
- Access shall be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., shall be returned or disabled.

Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization's premises.

An appropriately cleared and technically knowledgeable Staff member shall be present within the area where maintenance is being performed to ensure that security procedures are followed.

- If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.
- System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.

- Prior to maintenance, the information system is completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared, procedures identified in the System Security Plan shall be enforced to deny the maintenance personnel visual and electronic access to any Sensitive Information contained on the system.
- A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled “UNCLASSIFIED -- FOR MAINTENANCE ONLY” and protected in accordance with procedures established in the System Security Plan.

Processing of Sensitive Information shall only occur in approved areas. In addition:

- Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.
- All personnel granted unescorted access to the area containing the Information System shall have an appropriate security clearance.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO10.05, APO11.09-10, APO12.02, APO13.07, DSS01.05, MEA01.05, MEA02.11
 GDPR Article 25, 32
 HIPAA 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(c), 164.310(d)(1)
 ISO 27001:2013 A.8.3.3, A.11.1
 NIST SP 800-37 3.3, 3.6, 3.7
 NIST SP 800-53 MP-5, PE-2-5, SC-42(3)
 NIST Cybersecurity Framework PR.AC-1-2, PR.AC-4, PR.AC-6-7, PR.AT-1, PR.DS-5, PR.PT-1
 PCI 8.6, 9.1-4, 9.9

PHYSICAL SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Physical security is an essential part of an overall security plan. It forms the basis for all other security efforts, including data security.

II. Purpose

Physical security ensures that F2OnSite's Information Resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

III. Scope

This policy applies to all F2OnSite Staff responsible for the security of F2OnSite's facilities and related resources.

IV. Policy

Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g. electrical surges, extreme temperatures, spilled liquids). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Physical protection against natural disasters, malicious attack, or accidents shall be designed and applied.

Each Department is required to have a Facility Security Plan (Plan) which includes measures to safeguard Information Resources. The Plan shall describe ways in which all Information Resources are protected from physical tampering, damage, theft, or unauthorized physical access. Procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.

Physical and environmental security controls protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. F2OnSite's physical and environmental security program prevents interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data, information systems, and information processing facilities.

Physical controls and attestation mechanisms shall be designed to address legislative requirements. The results shall be shared with F2OnSite management and cloud computing tenants.

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing servers and data.

- Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
- Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
- Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference, or damage. Procedures shall monitor, control, and protect communications at external boundaries and at key internal boundaries of Information Systems.
- Equipment shall be correctly maintained to ensure its continued availability and integrity.
- Equipment, information, or software shall not be taken off-site without prior authorization.
- Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
- All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
- Users shall ensure that unattended equipment has appropriate protection.
- When leaving their work area, users shall ensure that their desk and work area is clear (clear desk) of papers and removable storage media. In addition, monitors shall be cleared (clear screen) to protect against unauthorized access to information or information systems. See the Clear Desk Policy for more information.
- Physical access controls address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.
- It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.
- Each individual that is granted access rights to a facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.

All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes. Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data as well as the risk to human life. Smoke, corrosive gases and high humidity from a localized fire can damage systems throughout an entire building. Security personnel must evaluate the fire safety of buildings that house systems.

Systems and the people who operate them need to have a reasonably well-controlled operating environment. Failures of electric power, heating and air-conditioning systems, water, sewage, and other

utilities will usually cause a service interruption and may damage hardware. F2OnSite Staff must ensure that these utilities, including their many elements, function properly.

Staff must be made aware that a building may be subjected to a load greater than it can support. Commonly, this is a result of an earthquake, explosion that displaces or cuts structural members, or a fire that weakens structural members.

While plumbing and roof leaks do not occur every day, they can be seriously disruptive. Staff must know the location of plumbing lines that might endanger system hardware and take steps to reduce risk (e.g., moving hardware, relocating plumbing lines, and identifying shutoff valves).

IT equipment must be marked with some form of identification that clearly indicates it is the property of F2OnSite. Refer to the Data Marking Policy for additional information in this area.

The Chief Security Officer shall ensure:

- Policies and procedures safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- Policies and procedures include controls such as locked doors, signs warning of restricted areas, surveillance cameras, alarms, property controls (property asset tag, engravings), and personnel controls (ID badges, visitor badges, escorts), security service or patrol of the facility.
- Policies and procedures specify how to document facility repairs and modifications.
- Policies and procedures specify all physical security components that require documentation.
- Policies and procedures identify special circumstances when repairs or modifications to physical security components are required such as when special staff members with special access (e.g. application administrators) are terminated.
- Procedures document the process to test data center environmental controls (e.g. electrical power, battery backups, and air conditioning) on a quarterly basis. Such activities shall be recorded in a log.
- Workstation physical safeguards restrict access only to authorized users.
- Procedures specify physical safeguards for workstations and other devices that access, receive, transmit, process, or store sensitive information.
- Procedures identify devices (e.g. workstations, desktops, laptops, tablets, smartphones, etc.) that are allowed to access systems containing sensitive information.
- Physical safeguards are effective at protecting workstations and other devices that access, receive, transmit, process, or store sensitive information.
- Procedures identify when additional physical safeguards are needed to protect workstations and other devices that access, receive, transmit, process, or store sensitive information.
- Access points such as delivery, loading, and other points where unauthorized persons could enter the premises are controlled, and, if possible, isolated from information processing facilities to avoid unauthorized access.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads and those responsible for information and physical security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO10.05, APO11.09-10, APO12.02, APO13.07, DSS01.05, MEA01.05, MEA02.11
GDPR Article 25, 32
HIPAA 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(c), 164.310(d)(1)
ISO 27001:2013 A.8.3.3, A.11.1
NIST SP 800-37 3.3, 3.6, 3.7
NIST SP 800-53 MP-5, PE-2-5, SC-42(3)
NIST Cybersecurity Framework PR.AC-1-2, PR.AC-4, PR.AC-6-7, PR.AT-1, PR.DS-5, PR.PT-1
PCI 8.6, 9.1-4, 9.9

PORTABLE COMPUTING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

II. Purpose

The purpose of this Policy is to establish the rules for the use of portable computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of information.

III. Scope

This policy applies to all F2OnSite Staff that utilize portable (mobile) computing devices and access F2OnSite Information Resources.

IV. Policy

Only IT Department approved portable computing devices may be used to access F2OnSite networks and Information Resources.

All mobile computing devices must be protected with a password required at the time the device is powered on. The password must meet the requirements of F2OnSite's Password Policy.

Sensitive data shall not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques per the Encryption Policy.

Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized. See the Wireless Access Policy for more information.

Non-F2OnSite computer devices that require network connectivity must conform to F2OnSite IT standards and must be approved in writing by the IT Department.

Unattended portable computing devices must be physically secured. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Laptops and other mobile devices that access F2OnSite's Network Infrastructure shall have active and up-to-date anti-malware and firewall software.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from portable computing devices which are generally higher-risk than non-portable devices (e.g., desktop computers).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO10.05, APO12.02, APO13.07, BAI02.05, BAI03.05, DSS01.05, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001:2013 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-1, ID.GV-4, ID.RA-4, PR.AC-1-4, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2

PRIVACY POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite may collect Personal Information from individuals and will collect Personal Information about Staff for various purposes, primarily relating to establishing and managing the employment or other work relationship between F2OnSite and its human resources. F2OnSite may also collect Personal Information from other sources including previous employers, work associates, personal references or other third parties to whom the Staff member has given permission to disclose the information.

F2OnSite shall identify the purposes for which Personal Information is collected at or before the time the information is collected.

II. Purpose

F2OnSite has a responsibility to inform Staff of the policies and practices for the management of Personal Information and will make these policies and practices understandable and easily available.

III. Scope

Consent requirements may vary depending upon circumstances and upon the type of Personal Information that F2OnSite intends to collect, use, or disclose. When determining whether a consent is required, F2OnSite will take into account the type of Personal Information collected, the sensitivity of the Personal Information, and the purposes for which F2OnSite will use the information. If consent is required, F2OnSite will determine the form of consent that is appropriate. Consent may be expressed, implied or deemed and may be obtained in person, by phone, by fax, by mail, e-mail, or via the Internet. Subject to our legal rights and obligations, F2OnSite shall seek consent to collect, use or disclose Personal Information for a new purpose.

IV. Policy

A. Individual Privacy Rights

Individuals (non-Staff) shall be permitted to take an active role in monitoring and protecting their Personal Information. An individual's privacy rights are grouped into the following major categories:

- Right to Know. F2OnSite shall inform individuals of the intent to collect Personal Information, the right to know what Personal Information is being or has been collected, where the data originated, how it will be used, and with whom it will be shared.
- Right to Consent. F2OnSite shall require the individual's opt-in consent for the use, disclosure, sale, or access to the individual's Personal Information. The individual may revoke consent at any time.
- Right to Prevent. F2OnSite shall inform individuals of the right to prevent F2OnSite from sharing their Personal Information with third parties.
- Right to Request. F2OnSite shall inform individuals of the right to request a copy of their Personal Information on file.
- Right to Deletion. F2OnSite shall inform individuals of their right to request F2OnSite remove Personal Information on file.
- Right to Pricing. F2OnSite shall inform individuals that our organization is prohibited from charging an individual a different price, or refusing service, even if the Individual exercised their privacy rights.

B. Staff Privacy Rights

F2OnSite Staff shall be informed of our intent to collect Personal Information, the right to know what Personal Information is being collected, where the data originated, how it will be used, and with whom it will be shared.

F2OnSite will compile and may disclose certain information about Staff to a limited number of third parties and those we are obliged to do so by law in order to administer staffing, compensation, benefits, and similar programs. F2OnSite may disclose Personal Information about its Staff in the context of providing references regarding current or former employees in response to requests from prospective employers.

Although F2OnSite will protect and limit the use of Personal Information about Staff that is disclosed to third parties, F2OnSite is not responsible for the subsequent uses or disclosure of the subject Personal Information by the third-party recipient such as government agencies.

C. Privacy Controls

Disclosure. F2OnSite shall, at or before collection, disclose to individuals or Staff:

- The categories of Personal Information to be collected and the purpose of collecting such information
- The categories of sources from which the Personal Information is collected
- The specific pieces of Personal Information the organization has collected
- The categories of Personal Information that may be shared and the purpose for sharing such information
- The categories of third parties with whom the Personal Information may be shared
- A list of categories of Personal Information shared in the preceding 12 months
- Whether third parties may collect Personal Information from different sources
- A description of the process for individuals and Staff to review and request changes to their Personal Information
- One or more designated methods for submitting verifiable requests

- The process through which the organization notifies the individual or Staff of material changes to the notice
- The effective date of the notice

Accuracy. F2OnSite shall take appropriate steps to ensure that Personal Information is accurate, complete, and up-to-date to minimize the possibility that inaccurate Personal Information is used.

Purpose. F2OnSite shall not use or disclose Personal Information for purposes other than those for which it was collected, except with the consent of the individual or if the use or disclosure is authorized by law.

Sharing. Personal Information collected in one business unit of F2OnSite may be shared with other business units of F2OnSite for the specifically identified purpose.

Requests. Subject to F2OnSite's legal rights and obligations, F2OnSite shall, upon receipt of a written request, inform the individual or Staff member of the existence, use and disclosure (including names and addresses of third parties) of his or her Personal Information over the past 12 months, and shall, subject to reasonable limitations, permit access to that information. F2OnSite shall respond to a request to access Personal Information within a reasonable time and no later than 45 days. Such requests shall be processed free of charge to the individual or Staff member.

Modifications. Subject to F2OnSite's legal rights and obligations, F2OnSite shall, upon receipt of a valid written request that demonstrates Personal Information is not accurate or complete, update the Personal Information as appropriate.

Opting out. F2OnSite shall refrain from asking for opting in consent for 12 months from the date an individual opts out. Individual opting out requests shall only be used for opting out and shall not be used for other purposes.

Age. F2OnSite shall not sell or rent the Personal Information of an individual under 16 years of age unless affirmatively authorized by the individual, age 13 to 16, or by a parent for individuals under the age of 13.

Web site. F2OnSite's Web Site Privacy Policy shall include individual privacy rights and considerations.

D. Security Controls

Risk management. The risk assessment, risk analysis, and risk treatment plan shall consider privacy related threats and controls to treat risks.

Practices. F2OnSite shall provide adequate safeguard practices to ensure the security of Personal Information, protect the Personal Information against loss or theft, and safeguard the Personal Information from unauthorized access, disclosure, copying, use or modification. Personal information shall be protected from electronic threats by the use of firewalls, intrusion detection, anti-virus, anti-spyware, passwords, and related security mechanisms.

Access. Only F2OnSite Staff with a business need to know, or whose duties reasonably so require, shall be granted access to Personal Information.

Minimum necessary. The collection of Personal Information shall be limited to the amount and type of information specifically required for an identified purpose.

Retention. Personal information shall only be kept only as long as necessary to satisfy the specified purpose. Files containing Personal Information are business records and, as such, the property of F2OnSite.

Physical security. Personal Information shall be stored in an access-controlled facility.

Monitoring. Monitoring and logging processes shall be used to ensure security controls and safeguards are operating as planned. Logs and alerts should be continuously monitored with appropriate action taken.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT EDM01.01, EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10
GDPR Article 24, 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.502(b)(1), ARRA 13404(b), ARRA 13405(a)
ISO 27001:2013 A.9.1.1, A.9.2.2, A.18.1.3-4
NIST SP 800-37 3.2, 3.4, 3.7
NIST SP 800-53 AC-3-4, AC-6, AC-21, AC-23, AU-9-10, Appendix F, Table F-1
NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RM-1, PR.AC-1-4, PR.AC-6, DE.DP-2
PCI 8.6, 9.1-4, 9.9

PROBLEM MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This Policy provides direction and guidance on managing problems that can disrupt F2OnSite's operations and/or adversely affect our image and reputation.

II. Purpose

This Policy is established to prevent and detect problems and incidents. Where incidents cannot be prevented, this Policy identifies processes to address the problems and minimize the impact on our organization.

III. Scope

This Policy applies to all individuals who manage and are responsible for F2OnSite's Information Resources.

IV. Policy

The Chief Security Officer (MGMT) shall ensure:

- Help desk or other teams are assembled to receive notice of problems and manage the process of investigating, responding to, and reporting of problems.
- Procedures and processes identify and respond to suspected or known problems, mitigate them to the extent practicable, measure harmful effects of known problems, document problems and their outcomes, collect evidence, and provide appropriate reporting to F2OnSite management.
- Response procedures list examples of problems and the appropriate responses for each.

A. Background

The primary objective of problem management is to prevent issues and incidents, reduce the likelihood of incidents, and minimize the impact of an incident. Problem management includes diagnosis of a problem to identify the root cause of an incident and determine the resolution.

Major problem management steps include:

- Problem detection – Help Desk captures relevant information such as person/system reporting the issue, date/time, systems involved, actions taken, etc.
- Problem analysis – determine the underlying issue, impact on the organization, and possible resolution. Document activities planned and taken.
- Problem logging – details of the problem are recorded so that a record and audit trail exists.
- Problem prioritization – problems are prioritized according to their impact on our organization. The problem frequency, likelihood, workarounds, extent, resources required, cost, and other factors help determine priority.
- Problem investigation and diagnosis – appropriate Staff investigate and diagnose the problem to assist in identifying relevant issues. Important steps include preparing a chronological list of events that triggered the problem, identifying the target/size (number of systems, departments, etc.) impacted, location(s), and possible and true cause(s).
- Problem History Data Base – the event is logged in a Problem History Data Base (Data Base). The Data Base is used to identify and reduce the likelihood of future similar events and to quickly resolve similar issues.
- Problem communications – Help Desk keeps all relevant parties updated on the status of the problem and expected resolution dates. Relevant parties include, but not limited to, the individual that reported the problem as well as the MGMT and upper management (if the issue has a major impact on the organization).
- Problem review – the MGMT ensures a periodic review of the Problem History Data Base is performed. Such review identifies opportunities to minimize future incidents and their impact on our organization.

B. Preventive Controls

The MGMT shall identify preventive controls that help prevent problems and incidents. When problems occur, preventive controls help contain and minimize the impact on business operations. Examples of preventive controls are listed below.

Only users with special training or a need for additional access shall be allowed to change system settings and install programs that are not operating system programs. For more information see the User Privilege Policy.

Network documentation helps F2OnSite adhere to industry best practices, reduce downtime and makes the troubleshooting process more efficient when problems arise. For more information see the Network Documentation Policy.

Before approving updates, System Administrators shall understand the addressed vulnerability, previous patches or system update required, programs affected by the change, and problems that may result as a result of the change. For more information see the System Update Policy.

Periodic backup copies of software and data shall be made, tested, and stored securely. The physical security of the removable media must be maintained with plans to allow recovery from unexpected problems. For more information see the Security Policy.

Hard drives that are not fully encrypted (e.g., have encrypted partitions, virtual disks, or are unencrypted) that connect to encrypted (e.g. USB drives) may be vulnerable to information spillage from the encrypted region into the unencrypted region. The hard drive's unencrypted auto-recovery folder may retain files that have been saved to the encrypted portion of the disk or USB. Full disk encryption shall be implemented to avoid this problem. For more information see the Encryption Policy.

Vendors play an important role in the support of F2OnSite hardware, software, and operations. Vendors can monitor and fine tune system performance, monitor hardware performance and errors, modify environmental systems, and reset alarm thresholds. For more information see the Vendor Access Policy.

Processes shall be in place to install and test all new/replacement software and hardware. Supervise all problem solving. Problem solving shall be supervised and documented. For more information see the Business Continuity Disaster Recovery Plan.

Staff shall follow approved procedures when dealing with copyright, trademark, and trade secrets. For more information see the Acceptable Use Policy.

C. Detective Controls

The MGMT shall identify detective controls that detect problems and incidents. When problems occur, early detection can help contain and minimize the impact on business operations. Examples of detective controls are listed below.

Compliance tracking shall be used to map programs and activities to standards established by the MGMT. Reports shall be generated and used to identify gaps or problems so that the appropriate corrective action can be taken. For more information see the Security Awareness and Training Plan.

Application logs help identify security incidents, establish baselines, provide information about problems and unusual conditions, assist with incident investigation, and help detect attacks. The MGMT shall identify application events and activities to monitored and logged. For more information see the Logging Policy.

The IT Department shall be responsible for establishing, communicating and enforcing department level practices and procedures that promote security. Account auditing shall identify accounts that no longer have authorized access to F2OnSite's Information Resources. The IT Department shall identify and correct problems caused on any network or system under their control. For more information see the IT Management Policy.

Resource monitoring and problem identification processes shall use audit trails to detect disk failures, over utilization of system resources, network outages, and similar events. Auditing systems shall consist of logging (collecting and recording events) and reporting (data analysis and reporting). For more information see the Audit Trails Policy.

Testing provides assurance that backups are complete and error free. Backups shall be tested to identify problems and issues related to the inability to restore from media. Such problems may include older media, poor quality, not properly stored, current backup software cannot read old backups, applications or data

were not stored on original backups, encryption or key management issues (can't read encrypted backups), etc. For more information see the Backup Plan.

The Emergency Action Applications Team shall participate in preparing and conducting tests at the Contingency Site. If a problem exists on how an application will operate at the Contingency Site, the Emergency Action Applications Team must prepare and document solutions for the problem. For more information see the Business Continuity Disaster Recovery Plan.

Effective privacy protection shall include robust mechanisms for assuring compliance with privacy principles and recourse for individuals who are affected by non-compliance with privacy principles. Processes shall include obligations to remedy problems arising out of failure to comply with privacy principles. For more information see the EU Privacy and Data Protection Policy.

D. Corrective Controls

The MGMT shall identify corrective controls that mitigate problems and restore operations. When problems occur, early correction can help contain minimize the impact on business operations. Examples of corrective controls are listed below.

The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem. For more information see the Audit Trails Policy.

Software manufacturers frequently provide bug fixes and software patches for known problems. In-house change control procedures shall developed to provide for adequate testing before making changes and for backing out the changes if problems are detected. Should bug fixes or software patches cause a failure of software or network services, the Contingency Site Coordinator shall take the appropriate action to correct the problem either by authorizing a manufacturer-provided "fix" or by designating that the software be returned to the version prior to loading the changes. Some of F2OnSite's applications packages were acquired from third-party sources and are maintained by those companies. These vendors can assist in correcting application problems. For more information see the Business Continuity Disaster Recovery Plan.

If a severe incident occurs, the Emergency Coordinator shall determine the severity of the problem and decide on the appropriate action. All recovery teams will be asked if they are aware of other information or circumstances that need to be considered. The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing schedule or anything else, before proceeding to carry out their individual team functions. This is important to ensure that all teams understand the key issues which will result in better coordination. The final activity of the recovery process will be a meeting and debriefing of the Readiness Team, all Coordinators, and Emergency Action Team Leaders concerning the activities of the recovery. The Emergency Coordinator is responsible to ensure that events, problems, solutions, etc., are documented. For more information see the Business Continuity Disaster Recovery Plan and Business Continuity Business Resumption Plan.

E. Training

The MGMT is responsible for ensuring that IT Department Staff have the proper training and appropriate problem management policies, procedures, plans and related documents. No less than annually,

awareness and refresher training shall be provided to maintain problem management readiness and competency. The MGMT may also arrange problem management exercises to test and evaluate Staff, related procedures, and the ability to respond to problems in a timely and effective manner.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Chief Security Officer, Company Management, Director of IT, Help Desk, and Security Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM01.03, EDM02.03, EDM03.07, EDM05.10, BAI09.04, DSS01.05, DSS03.05
 GDPR Article 30, 32
 HIPAA 1164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.312(b), 164.312(e)(2)(i), 164.312(e)(2)(ii)
 ISO 27001:2013 6.2, 7.5, A.16
 NIST SP 800-37 3.1, 3.2, 3.3, 3.4, 3.7
 NIST SP 800-53 AU-2, CP-2, IR-8, PL-2, PM-1, RA-3, SA-8
 NIST Cybersecurity Framework ID.AM-5, ID.BE-4, ID.RA-1, ID.RA-6, PR.PT-1, DE.AE-2
 PCI 1.1.1, 8.4, 10.8.1, A3.3.1.1

PROCEDURE TEMPLATE

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Policies provide management direction and guidance with the intention of influencing courses of action and decision making to ensure they are in line with F2OnSite's philosophy, goals and objectives and strategic plans. Procedures document a detailed description of the steps necessary to perform specific operations that comply with F2OnSite's policies and standards.

II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in F2OnSite's [Policy Name].

III. Scope

This procedure applies to all F2OnSite Staff who [Describe Scope: For example, manage F2OnSite's Information Resources.].

IV. Procedure

[Provide a detailed list of the steps taken, Staff that perform the actions, Information Systems involved, frequency, reports generated, responsibilities, reviews, approvals, etc. If any new Terms are used, ensure they are defined in the Terms and Conditions Policy.]

V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

VI. Distribution

This procedure is to be distributed to all F2OnSite Staff who [Describe Distribution].

Procedure History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial procedure release	D. Lauderback

References: [List applicable references below]

COBIT
GDPR
HIPAA
ISO 27001
NIST 800-41
NIST SP 800-53
NIST Cybersecurity Framework
PCI

PRODUCTION INPUT OUTPUT CONTROLS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

The production, input/output controls are the security procedures in place that support the operations of Information Systems.

II. Purpose

Strong, disciplined, and a clearly defined approach to production, and input and output controls helps ensure the confidentiality, availability and integrity of F2OnSite's Information Systems.

III. Scope

This policy applies to the IT Department and other individuals responsible for the security of F2OnSite's Information Resources.

IV. Policy

F2OnSite's IT Director is responsible for the security, accuracy and the reliability of Information Systems. IT application controls shall be used to ensure information confidentiality, availability, and integrity.

IT application controls refer to production and transaction processing controls, also known as input, processing, and output controls. IT application controls shall be automated (i.e., performed automatically by the systems) to ensure the complete and accurate processing of data from input through output.

The controls will vary based on the business purpose of the specific application. These controls may also help ensure the privacy and security of data transmitted between applications. The IT Director will identify application controls to be used and can include:

- Authentication - controls that provide an authentication mechanism in the application system.
- Identification - controls that ensure all users are uniquely and irrefutably identified.
- Completeness checks - controls that ensure all records were processed from initiation to completion.
- Validity checks - controls that ensure only valid data is input or processed.

- Authorization - controls that ensure only approved business users have access to the application system.
- Input controls - controls that ensure data integrity fed from upstream sources into the application system.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite's IT Department and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM04.09, APO01.03, APO01.11, APO12.02, APO12.07, DSS01.05, DSS03.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(d), 164.312(e)(2)(i), 164.312(e)(2)(ii)

ISO 27001:2013 8.1, 9.1, A.6.2.2, A.8.2, A.9, A.12.1.1

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 AC-16, CM-6, IA-5, IA-6, PE-5, SC-41, SI-4, SI-10

NIST Cybersecurity Framework PR.AC-1-4, DE.DP-2, RS.MI-2

PCI 6.5, A3.2.5

QUALITY ASSURANCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite's quality assurance and quality control programs are designed to monitor, evaluate, and improve the quality of our products and services.

II. Purpose

The purpose of this policy is to specify F2OnSite's commitment to maintain high quality work, the services we provide, our relationships with Staff, and ensure continuous improvement.

III. Scope

This policy applies to all F2OnSite Staff.

IV. Policy

The overall aim of a quality assurance program is to deliver the best service and products possible at a good value while ensuring continuous improvement. F2OnSite's quality assurance program improves business processes in a proactive manner to minimize variations or defects. Our quality control program includes reactive measures such as product or service quality testing.

F2OnSite shall maintain an effective and efficient quality assurance and quality control process planned and developed in conjunction with Department Heads. Outlined in a series of procedures, the quality assurance program is designed to eliminate deficiencies and inaccuracies and to ensure high quality standards.

F2OnSite Staff shall:

- Ensure that policies, procedures, and plans are developed and reviewed at least annually to ensure they reflect F2OnSite's values and support our mission
- Maintain a consistent work method without significant deviation and in accordance with F2OnSite policies, procedures, and plans
- Understand and identify customer (internal or external) needs and future requirements

- Establish work method Service Level Agreements (SLA) or metrics that can be measured and monitored
- Regularly monitor and measure the quality of work methods, outputs and outcomes with a view to ensuring high quality, best value, and continuous improvement
- Ensure corrective controls exist to keep work product and service delivery within acceptable limits
- Identify measures that can prevent a possible decrease in quality in addition to measures that restore a level of quality

Procedures shall be developed to ensure that a product or service measures up to standards. Where appropriate, training and testing shall be used to ensure Staff have the appropriate knowledge and skill sets needed.

Procedures shall track the quantity and types of defects produced by a specific process. The reported number of defects shall serve as a measure of the performance of quality assurance. The ultimate goal is to consistently reduce defects to minimum levels.

Total Quality Management (TQM) places emphasis on every department rather than singling out individual processes. TQM efforts begin and end with customer satisfaction. Customer feedback shall be considered along every step of a product or service lifecycle from initial conception through delivery to ensure that products and services meet customer requirements before delivery rather than adapting at a later stage.

A strategy for implementing F2OnSite's quality assurance and quality control programs using a Plan-Do-Check-Act (PDCA) lifecycle for quality management:

- Plan – ensure that quality assurance policies and procedures are in line with company initiatives and quality standards.
- Do – gain support from all levels of F2OnSite management and implement the quality assurance and quality control programs
- Check – regularly monitor and measure work products and service delivery, compare with requirements and identify variances
- Act – adjust business processes, refine policies and procedures as needed

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM05.10, APO06.04, APO11.10, APO14.10, BAI09.04, DSS01.05, MEA01.10
 GDPR Article 25, 32
 HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(6)(ii)
 ISO 27001:2013 8.1, 9.1, 10.1, A.5.1.1, A.9.4.3, A.12.1.3, A.12.4, A.15.2.1
 NIST SP 800-37 3.3, 3.5, 3.7
 NIST SP 800-53 CM-9, IA-5, IP-3, PM-23, SA-12, SA-15, SI-19
 NIST Cybersecurity Framework ID.BE-3, ID.BE-4, ID.RA-6, ID.SC-1, PR.DS-6, PR.IP-1, DE.DP-2
 PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

RANSOMWARE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Ransomware is a type of malicious software (malware) that can deny access to files or data. The software has different variations that may lock a computer or device or encrypt files. Typically the software demands payment using electronic currency. Controls are needed to ensure F2OnSite's Information Systems are protected against new and emerging types of malicious software.

II. Purpose

The purpose of this policy is to describe the requirements for managing risks related to Ransomware.

III. Scope

This policy applies to the Chief Security Officer.

IV. Policy

The Chief Security Officer shall ensure:

- The Risk Assessment, Risk Analysis, and Risk Treatment Plan identify Ransomware related risks and controls to address such risks. See the Risk Management Policy for more information.
- Policies, procedures, and tools are developed and maintained to prevent, detect, and take corrective actions to manage Ransomware related risks. See the Anti-Malware Policy for more information.
- Anti-virus software is installed at appropriate locations within organizational Information Systems including all systems commonly affected by malicious software (particularly personal computers and servers). Installed anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. See the Anti-Malware Policy for more information.
- Spam filters are implemented to reduce the likelihood Staff will click on e-mail links or download malware attachments to their local devices. See the E-mail Policy for more information.
- Backups are performed per the Backup Policy and Backup Plan.
- End users receive the appropriate security education and awareness training and such training address risks related to Ransomware. See the Security Awareness and Training Plan for more information.

- Social engineering security assessments evaluate the effectiveness of the Security Awareness and Training Plan. See the Audit Policy for more information.
- Malware actions (e.g. anti-malware software updates, definition updates, malware infections, Ransomware attacks, etc.) are logged with logs retained for one year to allow proper investigations into malware related incidents.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO13.07, APO14.10, BAI04.05, BAI09.04, DSS04.05, DSS04.07, DSS05.02, DSS05.07
GDPR Article 25, 32
HIPAA 164.308(a)(5)(ii)(B)
ISO 27001 A.12.2
NIST SP 800-37 3.1
NIST SP 800-53 AC-19, PL-8, SC-3, SI-2-4
NIST Cybersecurity Framework DE.CM-4-5, RS.RP-1, RC.RP-1
PCI 5.1-4

REMOTE ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

The purpose of this policy is to define standards for connecting to F2OnSite's network from any remote location. These standards are designed to minimize the potential exposure to F2OnSite from damages which may result from unauthorized use of F2OnSite Information Resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, and damage to critical F2OnSite Information Systems.

II. Purpose

This policy applies to all F2OnSite Staff with a computer used to connect to the F2OnSite network from a remote location. This policy applies to remote access connections used to do work on behalf of F2OnSite, including reading or sending e-mail and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, high speed Internet connectivity, Virtual Private Network (VPN), Secure Shell (SSH) and other forms of electronic connectivity to Information Systems.

III. Scope

This policy applies to all Staff that access F2OnSite's Information Resources from a remote location.

IV. Policy

Staff shall contact the IT Department for approved methods to remotely connect to F2OnSite's Information Systems. Staff shall review F2OnSite's Securing Information Systems Policy for details on protecting information when accessing the corporate network via remote access methods. Staff shall review the Acceptable Use Policy for the acceptable use of F2OnSite's Information Systems.

It is the responsibility of Staff with remote access privileges to F2OnSite's Information Systems to ensure that their remote access connection is given the same consideration as the user's on-site connection to F2OnSite.

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong password/phrase see the Password Policy. At no time should any F2OnSite Staff member disclose their login or e-mail password to anyone.

When accessing F2OnSite's Information Resources from a remote location, Staff shall ensure:

- F2OnSite's policies and procedures are followed.
- Friends and relatives do not have access to F2OnSite's systems and assets.
- Staff do not connect to other networks (excluding the Internet and an in-house personal network) at the same time they are connected to F2OnSite's systems.
- Only F2OnSite e-mail accounts are used for business related communications.
- All computers, mobile devices, etc. use up-to-date anti-malware software and an activated firewall (if available). Please refer to the Anti-Malware Policy and Mobile Device Policy for more information.

Personal equipment used to connect to F2OnSite's networks must meet or exceed the requirements of F2OnSite owned equipment for remote access. Staff who wish to implement non-standard remote access solutions to F2OnSite Information Systems must obtain prior approval from the IT Department.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.310(b)

ISO 27001 A.7.2.1, A.8.1.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-1-3

NIST Cybersecurity Framework PR.AC-3, DE.DP-2, RS.RP-1

PCI 2.3, 7.1-3, 8.1.5

REMOVABLE MEDIA POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

This policy governs the use of Removable Media used in F2OnSite's Information Systems.

II. Purpose

This policy is established to minimize risks related to removable media and Sensitive Information.

III. Scope

This policy applies to all Staff that access F2OnSite's Information Resources.

IV. Policy

The Chief Security Officer shall ensure:

- Policies and procedures govern device and media (including USB storage devices) controls. Procedures specify how devices are to be identified when there are multiple devices of the same type. Procedures ensure inventory logs of all media are implemented and maintained. Media inventories shall be conducted at least annually.
- Procedures classify media so the sensitivity of the data can be determined. Procedures specify the types of hardware and electronic media (e.g. hard drives, backup media, optical discs, digital memory cards) that must be tracked.
- Procedures store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Procedures ensure a review the media storage location's security at least annually.
- Procedures specify the record of the movements of hardware and electronic media and the person responsible for its movement. Procedures ensure management

approves any and all media that is moved from a secured area (especially when media is distributed to individuals). Procedures specify the receipt and removal of hardware and electronic media that contain sensitive information into and out of a facility, and the movement of those items within the facility. Media to be sent by secured courier or other delivery method that can be accurately tracked.

- Procedures for removal of sensitive information from electronic media before the media are available for reuse. Procedures specify situations where all sensitive information must be permanently deleted or when the electronic media should only be reformatted so that no files are accessible.
- Devices are configured to not auto-run content from removable media.

F2OnSite Staff may only use F2OnSite Removable Media. Removable Media may not be connected to or used in computers that are not owned or leased by F2OnSite without explicit permission of the IT Department.

Sensitive information shall be stored on Removable Media only when required in the performance of assigned duties or when providing information on Removable Media as required by state or federal agencies. When sensitive information is stored on Removable Media, it must be encrypted in accordance with F2OnSite's Encryption Policy.

Data shall be copied or stored on Removable Media only by authorized access in the performance of official duties. Removable Media containing sensitive information shall have an external label that is marked and dated. Such external labeling shall include any special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates). Refer to the Data Classification Policy and Data Marking Policy for more information.

Except for backups, access controls shall prohibit copying, moving or storing sensitive data on local hard drives and removable media.

Media containing information shall be protected against unauthorized access, misuse, or corruption during transportation. When in transit, sensitive data stored on Removable Media must not be left unattended, even temporarily, and must remain in an authorized employee's physical control at all times.

Physical and environmental protection controls shall be provided for Removable Media containing sensitive data. Removable Media containing sensitive data must be kept in a secure safe or a locked cabinet and returned to safe storage during breaks and at the end of each work day.

Staff shall adhere to the requirements outlined in the Disposal Policy when disposing of Removable Media.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO12.02, APO12.07, APO14.01-02, APO14.10, MEA03.01

GDPR Article 25, 32

HIPAA 164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii), 164.310(d)(2)(iii)

ISO 27001:2013 7.5.2, A.8.3, A.11.2.7, A.11.2.9

NIST SP 800-37 3.2, 3.4

NIST SP 800-53 3.11 (MP-1-8), MA-2, PE-6, PE-16, SC-28

NIST Cybersecurity Framework PR.AC-2, PR.PT-2, ID.RA-6, DE.CM-2, RS.MI-2

PCI 3.4, 9.1, 9.5-10

REPORTING VIOLATIONS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite Staff are responsible for notifying IT Help Desk or their supervisor if they suspect there has been a violation of an F2OnSite policy or if they suspect there may have been a security incident.

II. Purpose

Staff are a first line of defense and this policy helps ensure protection of F2OnSite Information Resources and their availability, integrity, and confidentiality.

III. Scope

This policy applies to all Staff that access F2OnSite's Information Resources.

IV. Policy

Every Staff member is responsible for ensuring that F2OnSite maintains the highest professional standards while protecting information confidentiality, integrity, and availability. Staff members are obliged to report any suspected violation of company policies. Reports can be made to any of the following departments as appropriate:

- Information Technology (IT)
- Human Resources (HR)
- Legal
- Executive Management

Staff shall not be disciplined or penalized for reporting honestly and in good faith. All reports shall be kept confidential except as necessary to conduct investigations.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM02.03, APO01.03, APO12.02, APO12.07, DSS01.05, MEA03.01, MEA04.11
GDPR Article 32, 33, 34
HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.314(a)(1)
ISO 27001:2013 9, 10.1, A.12.4, A.16.1.1-3
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 AU-6, CA-7, IR-6, IR-8, SI-2, SI-4
NIST Cybersecurity Framework DE.AE-1-3, PR.AT-1, DE.CM-1-2, RS.MI-2
PCI 9.9.3, A3.2.6.1, A3.3.1

RESILIENCE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Information Systems are critical to F2OnSite's business operations. Controls prevent disruption as well as provide the ability for F2OnSite to quickly restore services if they are disrupted. Resiliency is an important component of F2OnSite's risk management program.

II. Purpose

The purpose of this policy is to ensure appropriate controls are designed and implemented to provide F2OnSite with the ability to protect and recover quickly when an Information System is not able to provide service.

III. Scope

This policy applies to the Chief Security Officer (MGMT) and Risk Management Officer (RMO).

IV. Policy

Working together, the MGMT and RMO shall:

- Focus on capabilities supporting organizational missions or business functions.
- Identify processes that provide and maintain an acceptable level of service considering the threats and challenges to Information Systems.
- Ensure resilience includes the ability to withstand and recover from deliberate attacks, accidents, or events that occur naturally.

A resilient lifecycle shall be developed and maintained:

- Concept - Prioritize and tailor objectives, design principles, and limit the set of techniques and approaches to be used in solutions.
- Development - Use techniques and approaches to define alternative solutions, apply design principles to refine and analyze alternative solutions, develop capabilities to achieve the objectives.

- Production - Implement and evaluate the effectiveness of resiliency solutions, provide resources, or ensure that resources will be provided, to achieve the objective.
- Utilization - Monitor the effectiveness of cyber resiliency solutions, using capabilities to achieve objectives, reprioritize and tailor objectives as needed, and adapt mission, business, and/or security processes to address environmental changes.
- Support – Re-visit the prioritization and tailoring of objectives, use the results of monitoring to identify new or modified requirements, re-visit constraints on techniques and approaches, and modify or upgrade capabilities.
- Retirement - Prioritize and tailor objectives for the environment of operation, ensure that disposal processes enable those objectives to be achieved including modifying or upgrading capabilities of other systems as necessary.

The MGMT and RMO should ensure that risks are properly identified per the Risk Management Policy. Risk management is an on-going process by which F2OnSite Staff manage risks through a three-step process:

- Risk Assessment – Identify assets, threats to the assets, and vulnerabilities that exist as a result of the threats.
- Risk Analysis – For each risk, identify the likelihood and impact on our organization.
- Risk Treatment Plan – Develop controls and other safeguards designed to mitigate, eliminate, or transfer risks.

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. A summary of the departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans shall be reviewed by Executive Management on an annual basis to ensure that controls are sufficient and effective at treating risks.

F2OnSite's RMO shall ensure a formal and document Risk Management Framework has been established to manage risks related to Information Systems. The Risk Management Framework shall include:

- Categorize Information Systems
- Select security controls
- Implement security controls
- Assess security controls
- Authorize security controls
- Monitor security controls

The MGMT shall ensure:

- The Risk Assessment identifies scenarios that may result in a disruption to services.

- Security measures with preventive, detective, and corrective controls are implemented to ensure services are resistant to disruptions.
- Business continuity and disaster recovery processes restore operations within identified recovery point objectives and recovery time objectives.

When appropriate, the MGMT shall prepare and document an uncertainty analysis for the RMO. The uncertainty analysis shall consider a lack of sufficient information to determine the exact value of the elements of the risk model, including the threat frequency, safeguard effectiveness, or consequences.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Chief Security Officer (MGMT), Risk Management Officer (RMO), and executive management.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, APO09.05, BAI04.05, BAI04.07, DSS01.05, DSS03.05, MEA01.05
GDPR Article 32(b)
HIPAA 164.308(a)(1)(i)
ISO 27001:2013 9.3, 10.2, A.16.1, A.17
NIST 800-53 CP-2, 800-193 §2.3.1
NIST Cybersecurity Framework ID.BE-5, PR.IP-9-10, DE.DP-2, RS.RP-1, RC.RP-1
PCI 6.1

RISK ASSESSMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Risk assessments help identify business processes that are of high priority and importance to the organization so the proper controls can be implemented to reduce risks to acceptable levels.

II. Purpose

Information Resources are critical to maintaining F2OnSite's business operations. This policy ensures sufficient controls and resources are allocated to supporting and managing IT and its use within F2OnSite.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite's Information Resources.

IV. Policy

A. Risk Assessments

Risk assessments identify F2OnSite Information Resources and related threats and vulnerabilities. The accompanying risk analysis identifies the impact on our organization and provides recommendations for treating risks.

To properly secure and protect F2OnSite's Information Resources, a significant amount of design, planning, and implementation expertise is required to ensure that the proper level of controls are designed and implemented. While preparing and conducting a risk assessment, the following best practices or approaches should be considered.

F2OnSite's Risk Management Officer (RMO) shall first define the risk assessment's goals and objectives. Aligning these goals and objectives with the organization's

business drivers allows the organization to prioritize and focus on critical systems and assets.

F2OnSite staff shall identify and inventory important Information Resource assets and related components. Without an accurate inventory of infrastructure components and IT assets, an asset valuation, criticality, or importance evaluation cannot be performed.

Depending on the accuracy and availability of inventory documentation and asset valuation data (for example, capital dollars spent on hardware, software, integration, maintenance, staff salaries, G&A overhead), F2OnSite Staff should conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine which IT infrastructure components and assets are most important to the organization (either in monetary value or importance value).

Depending upon the scope of the risk assessment, F2OnSite management may or may not be faced with a limited budget to conduct a thorough risk and vulnerability assessment. In some cases, the organization may limit the scope to mission-critical IT infrastructure components and assets only.

The risk assessment shall identify assets, threats to the assets, vulnerabilities that exist as a result of the threats, and likelihood of the event. Charts or other documents shall describe how sensitive information is created, received, maintained, transmitted, and flows through the organization. Such documentation shall consider and identify:

- Less obvious sources of sensitive information including mobile devices.
- External sources including vendors, consultants, and other third party service providers that create, receive, maintain, or transmit sensitive information.

For third party service providers, at a minimum, the risk assessment shall:

- Be performed on an annual basis or more frequently if major changes occur to the environment or services performed.
- Identify compliance objectives and control requirements.
- Identify risks related to business continuity, capacities, and dependent services.

B. Risk Analysis

After the assets, threats, and vulnerabilities have been identified, the RMO shall ensure a risk analysis identifies the impact on F2OnSite's Information Resources. By aligning the potential risks, threats, and vulnerabilities to the prioritized assets, management can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities that are known.

The risk analysis shall include a Risk Treatment Plan that identifies how each of F2OnSite's risks can be managed:

- Mitigate – implement controls to reduce risks to an acceptable level.
- Transfer – transfer risks to another entity (usually through insurance).
- Avoid – change the business model to avoid or eliminate the risk if the risk cannot be reduced to an acceptable level or transferred to another entity.
- Monitor – acknowledge the risk and monitor to ensure the risk remains within acceptable limits.

C. Risk Treatment Plan

The Risk Treatment Plan shall include a prioritized list of assets, related vulnerabilities, and preventive, detective, and corrective controls that manage risks. The prioritized list helps align allocation of funds based upon criticality of the asset and related risks.

To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be located away from locations subject to high probability environmental risks.

Redundant equipment shall be located a reasonable distance away from primary systems.

For third party service providers, the risk analysis and risk treatment plan shall:

- Identify measures in place to protect Sensitive Information and provide services as outlined in the agreement with the service provider.
- Evaluate risks and ensure controls are in place to treat risks.
- Identify gaps from compliance objectives and control requirements. Make service provider aware of such gaps and take appropriate actions necessary.

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. The risk assessment, risk analysis, and risk treatment plan shall be reviewed on an annual basis to ensure that controls are sufficient and effective at treating risks.

The Chief Security Officer (MGMT) shall ensure:

- Security measures protect electronically transmitted sensitive information is not improperly modified without detection.
- The risk assessment identifies scenarios that may result in modification to sensitive information by unauthorized sources during transmission.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, APO01.03, APO03.06, APO12.02, APO12.07, APO13.07,
DSS05.02
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
ISO 27001:2013 6.1.2, 6.1.3, 8.2, 8.3, 9.3
NIST SP 800-37 3.2, 3.5, 3.7
NIST SP 800-53 3.17 (RA-1-9), SI-2, SI-4
NIST Cybersecurity Framework ID.RA-1-6, ID.RM-1, ID.SC-4, DE.CM-1-6, RS.RP-1,
RS.MI-2
PCI 6.1, 10.6.2, 10.8.1, 12.2

RISK MANAGEMENT POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Risk management is an on-going process by which F2OnSite Staff manage risks through a three-step process:

- Risk Assessment – Identify assets, threats to the assets, and vulnerabilities that exist as a result of the threats.
- Risk Analysis – For each risk, identify the likelihood and impact on our organization.
- Risk Treatment Plan – Develop controls and other safeguards designed to mitigate, eliminate, or transfer risks. It is important to treat risks in a cost effective and efficient manner.

II. Purpose

This policy establishes the framework for a formal risk management program by establishing responsibility for risk identification, analysis, and risk treatment. Risk management is an enterprise-wide activity that applies to all F2OnSite departments.

III. Scope

This policy applies to all Staff that access F2OnSite's Information Resources.

IV. Policy

Risk is the potential that a threat will exploit one or more asset vulnerabilities and result in a loss or failure to achieve an objective. At F2OnSite, risk management is the process of identifying, analyzing, and the use of safeguards and controls to treat risks.

Where possible, F2OnSite shall modify or eliminate conditions and practices which may cause loss. Where risk cannot be eliminated or reduced, it shall be monitored to ensure it remains within acceptable levels.

Risk management is an important component of F2OnSite's Resilient Policy.

A. Executive Management Responsibilities

Executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization. A summary of the departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans shall be reviewed by Executive Management on an annual basis to ensure that controls are sufficient and effective at treating risks. Executive Management may determine that the risks are acceptable given the kind and severity of known risks and unknown risks from the Chief Security Officer's uncertainty analysis.

B. Risk Management Officer Responsibilities

Risk Management Framework

F2OnSite's Risk Management Officer (RMO) shall ensure a formal and document Risk Management Framework has been established to manage risks related to Information Systems. The Risk Management Framework shall include:

- Categorizing Information Systems
- Selecting security controls
- Implementing security controls
- Assessing security controls
- Authorizing security controls
- Monitoring security controls

Categorize. Information Systems shall be categorized based upon the potential impact to the organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories shall be used in conjunction with vulnerability and threat information in assessing the risk to an organization. The security category of an Information System shall consider the confidentiality impact, integrity impact, and availability impact where the impact is classified as Low, Medium (Moderate), High, or Not Applicable. When determining the impact level of an information system the RMO shall consider the different types of information that are processed, stored, or transmitted by the information system, the impact values (Low, Medium, High, Not Applicable), the information system security categorization, that is, the highest impact value for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system, Determine the overall impact level of the information system from the highest impact value among the three security objectives in the system security categorization.

Select. An applicable security control baseline shall be selected based on the results of the security categorization. To adequately mitigate risk is an important task that requires a fundamental understanding of F2OnSite's mission/business priorities, the mission and business functions the Information Systems support, and the environments of operation where the systems reside. In preparation for selecting and specifying the appropriate security controls for organizational Information Systems and their respective environments of operation, the RMO shall first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. The RMO can employ a requirements definition approach or a gap analysis approach in selecting security controls and control enhancements to supplement initial baselines. The RMO shall document significant risk management decisions in the security control selection process so that Executive Management can have access to the necessary information to make informed authorization decisions for organizational information systems. Maintaining a record of security control selection and control status can be addressed in one or multiple documents or plans. There may be situations in which organizations cannot apply sufficient security controls within their information systems to adequately reduce or mitigate risk (e.g., when using certain types of information technologies or employing certain computing paradigms). Therefore, the RMO shall document alternative strategies to prevent organizational missions/business functions from being adversely affected. Once the impact level of the information system is determined, organizations begin the security control selection process. After selecting the applicable security controls, organizations initiate the tailoring process to modify appropriately and align the controls more closely with the specific conditions within the organization (i.e., conditions related to organizational missions/business functions, information systems, or environments of operation). The tailoring process includes:

- Identifying and designating common controls in initial security control baselines.
- Applying scoping considerations to the remaining baseline security controls.
- Selecting compensating security controls as needed.
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements.
- Supplementing baselines with additional security controls and control enhancements, if needed.
- Providing additional specification information for control implementation, if needed.

Implement. The protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security controls. When considering security controls, the RMO shall consider that F2OnSite is responsible and accountable for the information security risk incurred by the use of services provided by external third party service providers. Such risk shall be addressed by incorporating terms and conditions in the agreements with the external service providers. RMO baseline

security control tailoring actions can include: identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning specific values to security control parameters, supplementing initial baselines with additional security controls or control enhancements, and providing additional information for control implementation. The set of security controls must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, and other organizations based on the organizational risk tolerance. The RMO may find it necessary to employ compensating security controls. Compensating controls may be employed when management assesses and accepts the risk associated with implementing compensating controls in organizational information systems.

Assess. The RMO shall ensure security controls are assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Two fundamental components affecting the trustworthiness of information systems are security functionality and security assurance. Security functionality is typically defined in terms of the security features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. For more information on assessing security controls please see the Audit Policy, Audit Trails Policy, Change Management Policy, and Logging Policy.

Authorize. Executive Management shall authorize Information System operation based on a determination of risk to organizational operations and assets, individuals, and other organizations resulting from the operation and use of the Information System and the decision that this risk is acceptable.

Monitor. The RMO shall ensure monitoring of the security controls in the Information System and environment of operation on an on-going basis to determine control effectiveness, changes to the system/environment, and compliance to policies, legislation, and standards. For more information on security controls see Security Controls Review Policy. Security controls shall be carefully reviewed and revised periodically to reflect:

- Experience gained from using the controls.
- Control effectiveness.
- Changes to the system/environment.
- Compliance to policies, legislation, and standards.
- Changing security requirements.
- Emerging threats, vulnerabilities, and attack methods.
- Availability of new technologies.

Risk Management Processes

An effective risk management process identifies, mitigates as deemed necessary, and monitors on an on-going basis, risks arising from its information and Information Systems. Risk management processes shall be integrated throughout the organization to effectively address mission/business concerns. A three-tiered approach shall be employed that addresses risk at the organization level, mission/business process level, and the information system level.

The RMO's responsibilities include:

- Policies – Developing, implementing, and maintaining risk management policies, procedures, and guidelines.
- Management – Managing the risk management program that includes Risk Assessments, Risk Analysis, and Risk Treatment Plans.
- Approval – Approving departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans.
- Security – Forwarding departmental Risk Assessment, Risk Analysis, and Risk Treatment Plans to the Chief Security Officer for review and approval.
- Reporting – Provide necessary reporting to F2OnSite's Executive Management.

The Risk Management Officer shall review department head Risk Assessments, Risk Analysis, and Risk Treatment Plans to ensure:

- The Risk Assessment produces meaningful output that reflects what is truly important to the Company.
- Asset valuation appears to be appropriate and includes the value of information, software, personnel, hardware, and physical assets (e.g. data centers). The value of an asset consists of its intrinsic value as well as the consequences of loss of asset availability, confidentiality, and integrity.
- For systems under consideration or development, risks related to existing F2OnSite's systems.
- Security controls have been identified and reduce risk to acceptable levels. Although there is flexibility in how the Risk Assessment is conducted, the process of treating risks has greater flexibility than the sequence of events conducted in a Risk Assessment.

C. Department Head Responsibilities

1. Risk Assessment

Each Department Head shall ensure that a risk assessment is performed that identifies departmental and, where appropriate, organizational assets, owners of the assets, and opportunities. The risk assessment shall identify threats to the assets and

vulnerabilities that exist as a result of the threats. The Risk Assessment shall be performed on an annual basis and updated as needed. Refer to the Risk Assessment Policy for more information.

2. Risk Analysis

After the assets, threats, and vulnerabilities have been identified, Department Heads shall conduct a risk analysis that evaluates the likelihood of vulnerabilities and impact on the department and organization given the value of the specific asset and/or related resources. Department Heads shall consider the impact or lost value if the asset has been lost, disclosed, or compromised. By aligning the potential risks, threats, and vulnerabilities to the prioritized assets, Department Heads can make sound business decisions based on the value or criticality of that IT asset and the potential risk, threats, and vulnerabilities.

3. Risk Treatment Plan

Department Heads shall prepare a Risk Treatment Plan that identifies how each of the risks can be managed:

- Mitigate – implement controls to reduce risks to an acceptable level.
- Transfer – transfer risks to another entity (usually through insurance).
- Avoid – change the business model to avoid or eliminate the risk if the risk cannot be reduced to an acceptable level or transferred to another entity.
- Monitor – acknowledge the risk and monitor to ensure the risk remains within acceptable limits.

The Risk Treatment Plan shall include a prioritized list of assets, related vulnerabilities, and preventive, detective, and corrective controls that manage risks. The prioritized list helps align allocation of funds based upon criticality of the asset and related risks. The Risk Treatment Plan shall identify specific tasks (Risk Task List), resources required, and estimated completion dates.

Department Heads shall consider activities and controls that help mitigate risk. Consult with appropriate security Staff (IT, MGMT, physical security) to identify appropriate controls to treat risks. When selecting the appropriate controls, the following factors must be considered:

- F2OnSite policies and procedures, compliance requirements, and legislation
- Technical requirements
- Safety, reliability, and quality requirements
- System performance requirements

To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be located away from locations subject to high probability environmental risks. Redundant equipment shall be located a reasonable

distance away from primary systems. For cloud computing services the risk analysis and risk treatment plan shall:

- Manage risk as defined in the master agreement or industry best practices and standards.
- Identify security measures in place to protect sensitive information.

Department Heads shall:

- Monitor Risk Task List progress and update the Risk Treatment Plan as necessary.
- Submit the Risk Assessment, Risk Analysis, and Risk Treatment Plan to the Risk Management Officer for review and approval.

D. Chief Security Officer Responsibilities

The MGMT shall ensure the Risk Assessment identifies scenarios that may result in modification to sensitive information by unauthorized sources during collection, storage, and transmission. Security measures shall ensure sensitive information is not improperly modified without detection.

When appropriate, the MGMT shall prepare and document an uncertainty analysis for the Risk Management Officer. The uncertainty analysis shall consider a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads, the Risk Management Officer, and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, APO01.03, APO03.06, APO12.02, APO12.07, APO13.07,
DSS05.02
GDPR Article 24
HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
ISO 27001:2013 6.1.2, 8.2
NIST SP 800-37 2.2, 3.1-7
NIST SP 800-53 3.17
NIST Cybersecurity Framework ID.RA-1-6, ID.RM-1, ID.SC-4, DE.CM-1-6, RS.RP-1,
RS.MI-2
PCI 6.1, 12.2, PCI Software Security Framework

ROUTER SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Routers and switches are networking devices that send and receive data packets between computer networks and devices.

II. Purpose

This policy describes router security configurations to help minimize and control risks related to the connectivity and availability of F2OnSite's Information Resources.

III. Scope

This policy applies to all Staff that manage F2OnSite's network and communications systems.

IV. Policy

Every router and switch deployed in the F2OnSite network must be appropriately configured and meet configuration and security requirements.

Access controls shall be used to provide separate authentication, authorization, and accounting services.

Configurations shall prohibit direct public access between public networks (e.g. Internet) and any Information Resource containing sensitive information. Configurations, access control lists, and other network filtering technology must be used to limit network access to devices that store sensitive data. Configurations shall restrict all traffic, inbound and outbound, from untrusted networks (including wireless) and hosts and specifically deny all other traffic except for necessary protocols.

Local user accounts shall not be configured on the router. To prevent unauthorized changes, the device shall be protected using a password available from the IT Director.

Access rules shall be implemented and maintained per business needs and as approved by the IT Director.

Unless otherwise approved by the IT Director, routers shall be configured to disallow the following:

- IP directed broadcasts.
- Incoming packets at the router sourced with invalid addresses.
- TCP small services.
- UDP small services.
- All source routing.
- All web services running on router.

Each router must have the following statement posted in clear view: UNAUTHORIZED ACCESS PROHIBITED. Staff must have explicit permission to access or configure this device. All activities performed on routers shall be logged.

Unless there is a secure tunnel protecting the entire communication path, Telnet shall not be used to manage a router. When routers are remotely configured, Secure Shell (SSH) is the preferred management protocol.

IT security Staff shall ensure:

- Formal router hardening procedures are in place.
- Formal testing procedures are followed whenever configurations change.
- Router passwords are long and complex. Default passwords and configurations are changed on all routers.
- Routers are patched and updated in a timely manner. Documentation and procedures ensure that software updates and maintenance procedures are performed by authorized personnel.
- Routers are under support contract with appropriate response time guarantees and/or replacement routers are immediately available.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Staff that manage F2OnSite's routers and switches.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(4), 164.312(a)(1)
ISO 27001:2013 6.1.3(b), A.9.1, A.9.4.1, A.12.1, A.12.4, A.12.6, A.13.1.3
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 AC-4, RA-3, RA-5, SC-7, SI-2, SI-5
NIST Cybersecurity Framework ID.RA-1, PR.AC-3, PR.AC-5, PR.DS-1-2, DE.DP-2, RS.RP-1
PCI 1.1-3, 1.5, 11.1

SECURE SOFTWARE DEVELOPMENT LIFECYCLE POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Implementing sound software development techniques with proven security strategies helps F2OnSite manage its risks throughout the entire software lifecycle from initial inception through final disposition of an application.

II. Purpose

This policy describes the requirements for securely developing, implementing, acquiring, and managing the software development life cycle.

III. Scope

This policy applies to all Staff that provide and manage software development services.

IV. Policy

A. Software Development Lifecycle

F2OnSite's IT Department management is responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, SDLC should address the following ten areas:

1. Feasibility study
2. Risk assessment
3. User requirements
4. Systems design
5. Programming or acquire software (development/acquisition)
6. Quality assurance
7. Documentation
8. Systems testing and acceptance
9. Installation

10. Maintenance through disposal

Information security must be integrated into new application and systems development from their inception and throughout the development lifecycle. The development lifecycle is defined as a period that begins with conception of a new development project and ends with retirement or removal of the developed software from all active use.

B. Roles and Responsibilities

The Chief Security Officer (MGMT) are responsible for:

- Ensuring that security controls are developed to manage and reduce software related risks throughout its lifecycle.
- Ensuring software development projects include security in all stages of the lifecycle phases.
- Assist application developers and data owners in identifying security requirements for each lifecycle phase.

Data Owners are responsible for:

- Identifying sensitive information.
- Making application development staff aware of sensitive information and where it is used.

Application Developers are responsible for:

- Understanding and defining the security requirements for sensitive data.
- Understanding each phase of the software development lifecycle and the security controls required at each phase.
- Documents security controls required at each phase.

C. Secure Software Development Lifecycle Procedures

Specific security requirements shall be followed at each phase of the software development lifecycle.

1. Feasibility

The Chief Security Officer shall review requests that deal with sensitive information to ensure that proper security controls are considered during the feasibility study.

2. Risk assessment

The Risk Management Officer shall perform a preliminary risk assessment to ensure all material risks have been identified. The risk assessment shall include a sensitivity assessment that evaluates the sensitivity and criticality of the information to be

collected, stored, and processed. The risk assessment shall consider privacy issues, compliance requirements, and system continuity.

3. User requirements

Systems Analysts shall review system requirements and prepare user requirements, including the need to implement security controls that maintain information confidentiality, integrity, and availability.

4. Systems design

Systems Analysts will design the proposed system, incorporating security controls such as identification and authentication, access rights, logging and monitoring systems, encryption controls, and other specific security methodologies.

5. Programming or acquire software (development/acquisition)

Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and comply with applicable regulatory and business requirements. Programmers and software developers shall code applications using secure coding techniques that validate input fields, encrypt sensitive data, restrict access by need to know, etc. Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data. If the software was acquired, the IT Department shall ensure the application meets security requirements and, as much as possible, adheres to internal security development standards.

Developers shall be trained in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Applications shall be based on secure coding guidelines (see Open Web Application Security Project) that protect against attacks (e.g. injection, access controls, information disclosure, buffer overflow, input validation, cross site scripting, etc.), error handling, and other related secure coding techniques.

For public-facing web applications, F2OnSite shall address new threats and vulnerabilities on an on-going basis and ensure these applications are protected against known attacks by:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.
- Periodic independent audits performed annually or after a major software upgrade/release. See Audit Policy for more information.

6. Quality assurance

Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. The development team must ensure that software security features are properly coded and enabled.

7. Documentation

Documentation shall include procedures to restrict access to systems based upon prior authorization.

8. Systems testing and acceptance

Test data shall be carefully selected, protected, and controlled. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as:

- Fit for purpose - the product should be suitable for the intended purpose, and
- Right first time - mistakes should be eliminated prior to release.

Processes shall test security functionality prior to software release with security testing performed under conditions as close to production conditions as possible.

Data Owners shall review test results and provide approval prior to moving new software or software updates into production. Data Owners shall also review and approve data migrations from one application or system to another.

9. Installation

There shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system, while the development, and test environments maximize software development productivity.

- Software development staff must not be permitted to have access to production systems and related data.
- Development systems must not contain sensitive or confidential information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.
- Software debugging code must be removed before programs are placed into production.

IT Department's operations staff will move programs from development into production. Software developers shall not be permitted to move programs into the production environment.

The IT Department's operations staff shall complete any required security activities (logging, anti-malware scanning, encryption security certificates, etc.). Additional actions required can include changes to backup procedures, user training, work flows, etc.

10. Maintenance through disposal

Access to program source code shall be restricted to authorized personnel on a need to know basis. Procedures shall be developed to control the risks related to systems development access to production systems during emergencies (program aborts, etc.).

Upon software end of life and final disposition of the application, the following procedures shall be followed:

- Data Owner gives permission to terminate the application.
- IT department identifies retention requirements for software and data and ensures appropriate backups are stored in a secure location.
- IT Department operations staff securely removes or destroys the application and related code.
- IT Department operations staff ensures secure disposal of hardware and software according to the Disposal Policy.
- IT Department operations staff ensures disposition of licensed software meets requirements of the software license or other relevant agreements.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Staff that provide and manage software development and programming services.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT APO01.03, APO01.11, APO05.05, APO12.07, APO13.07, BAI03.05, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(2)
ISO 27001:2013 5.2, 6.2, A.14
NIST SP 800-37 3.2, 3.4
NIST SP 800-53 PL-2, PL-7, PL-8, SA-3, SA-4, SA-15, SA-17
NIST Cybersecurity Framework ID.AM-6, ID.GV-3-4, ID.RA-6, PR.IP-2-3, PR.MA-1
PCI 6.1-7

SECURING INFORMATION SYSTEMS POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Information and physical security help protect F2OnSite's Information Resources and ensure system confidentiality, availability, and integrity.

II. Purpose

This policy helps protect F2OnSite's assets and ensures our ability to continue business operations.

III. Scope

This policy applies to all Staff that use F2OnSite's Information Resources.

IV. Policy

Security rules and procedures protect important assets and support the overall F2OnSite (Company) mission. Through selecting and applying appropriate safeguards, security helps the Company's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Company Staff must understand both their organizational mission and how each information system supports that mission. After a system's role is defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the Company's mission.

The following security mechanisms shall be implemented to ensure information security and protect against data leakage through e-mail, social networks, and instant messaging applications.

Technologies such as fingerprinting shall be employed to ensure sensitive information can't be copied, printed, or e-mailed. Sensitive information shall not be copied, moved,

or stored onto local hard drives or removable electronic media unless explicitly authorized for a defined business need. Products shall be used to protect against data leakage:

- Data loss prevention (DLP) identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.
- Network based DLP solutions shall scan network traffic such as e-mail and instant messages for sensitive data.
- Endpoint DLP products shall tag and monitor sensitive data on servers, desktops, mobile devices, and other technologies that store data.
- Discovery DLP solutions shall locate and identify sensitive data.

Access to systems with shared network infrastructure shall be restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between the organizations.

A. Information Systems Risk Management

Information systems control virtually all of Company's major record-keeping functions. Risks are created by the unique nature of computers themselves. By concentrating information in one location, Company increases its risk of loss or damage. Another risk is access to information from remote locations. Company's information systems must be able to positively identify the user, as well as ensure that the user is only able to access information and functions that have been authorized.

Security personnel must evaluate the costs and benefits of security in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. Security must be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular information system. Security benefits do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software.

Staff shall refer to the Risk Management Policy to ensure proper steps are taken to identify and reduce risks to acceptable levels.

B. Information System Life Cycle

F2OnSite's IT Department is responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). Please refer to the Secure Software Development Lifecycle Policy for more information.

The disposal of hardware, software, and information requires special consideration. Refer to the Disposal Policy, Encryption Policy, Data Retention Policy, and Removable Media Policy for more information.

C. Audit and Monitoring Techniques

Where possible, the MGMT shall use Certified Information Systems Auditors to audit the security controls of F2OnSite's Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources. Refer to F2OnSite's Audit Policy for more information.

Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing F2OnSite's Information Resources. Audit trails can also be used as an incident detection and response mechanism. Refer to the Audit Trails Policy for more information.

D. General Information Systems Security Procedures

F2OnSite recommends common-sense protective measures to reduce the risk of loss, damage, or disclosure of information. The following guidelines identify Information Systems controls that assure that the system is properly used, resistant to disruptions, and reliable.

Access to information

- Use – users are a first line of defense and shall follow safe computing practices as outlined in the Acceptable Use Policy.
- Passwords – passwords are a key component to system security. Refer to the Password Policy for more information.
- Logon attempts – users shall be locked out after five consecutive invalid logon attempts within a 24 hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID.
- Inactivity – users shall be automatically logged off after 15 minutes of inactivity.
- Screen savers - protected screen savers are required and shall be activated after 15 minutes of inactivity.
- Inactive IDs. User IDs that are inactive on the system for a period of three months must be disabled.
- Clear desk – Staff shall ensure sensitive information remains secure by clearing their desks when they will be away from their office, positioning monitors to prohibit unauthorized viewing, etc. See the Clear Desk Policy for more information.
- Media – media must be handled according to Removable Media Policy requirements.

- Data storage – computers and handheld devices contain hard drives and non-destructive memory that may contain sensitive information. Refer to the Encryption Policy, Mobile Device Policy, Smartphone Policy, and Wearable Computing Policy for requirements to keep unauthorized individuals from accessing such data.
- Third party access – prior to granting individuals physical or logical access to information resources, agreements with staff, third party users, and customers shall be in place and include responsibility for information security. Refer to the Third Party Service Providers Policy for more information.

Communications and operations

- Diagnostic ports – physical and logical access to diagnostic and configuration ports shall be controlled. Refer to the Network Configuration Policy and Physical Access Policy.
- Border routers – border routers may be used to filter traffic and protect against spoofed IP addresses.
- Firewalls – firewalls shall protect the network and limit traffic to only approved activities. For more information see the Firewall Policy.
- Location – access to Information Resources may be based upon physical or logical location. Similarly, users can be restricted based upon network addresses (e.g., internal users may be permitted greater access than those from outside the organization).
- Time – time and day restrictions may be used to limit access to data (e.g. access to personnel files may only be allowed during normal working hours).
- Transaction - transaction based access criteria can be used. For example, access to a particular account could be granted only for the duration of a transaction. When completed, the access authorization is terminated.
- Management – networks shall be managed and controlled to protect information in systems and applications.
- Services - only network ports, protocols, and services listening on a system with validated business needs, shall be running on each system. Host-based firewalls or port-filtering tools on end systems shall apply a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Service levels – security mechanisms, service levels, and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

- Segments – groups of information services, users, and information systems shall be segregated on networks.

Information security protection

- Access – access controls enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. IT security Staff shall protect information stored on systems with file system, network share, claims, application, or database specific Access Control Lists (ACL). ACLs are a register of users (e.g. groups, machines, processes) permitted to use a particular system resource and the types of access they have been permitted.
- Account management – policies and procedures shall manage the process of creating, monitoring, controlling, and removal of accounts. Refer to the Account Management Policy for more information.
- Acquisitions – only hardware or software acquired through F2OnSite's approved policies and procedures may be installed. Refer to the Acquisitions and Procurement Policy.
- Authentication data – Information Systems must protect authentication data as it is entered including suppressing the display of the password as it is entered, and orienting keyboards away from view.
- Backups – backups protect against accidental or deliberate destruction of data. Refer to the Backup Policy for more information.
- Change – change detection systems (e.g. file-integrity monitoring tools) shall alert personnel to unauthorized modification of critical system files, configuration files, or content files. Such systems shall be configured to perform critical file comparisons at least weekly. Note: For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by IT security Staff. IT security Staff shall implement a process to respond to any alerts generated by the change detection solution.
- Confidentiality – the requirements for non-disclosure (e.g. confidentiality agreements) reflect F2OnSite's need for to protect data and operational details. Such requirements shall be identified, documented, and reviewed at planned intervals.

- Configurations – Staff must protect data by implementing and maintaining authorized hardware and software configurations. Refer to the Network Configuration Policy, Server Hardening Policy, and Workstation Hardening Policy for more information.
- Denial of Service – a Risk Assessment shall identify Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack threats. A Risk Analysis shall identify the likelihood of the event and impact on the organization. Preventive, detective, and corrective controls shall be identified and implemented as needed.
- Intrusions – intrusion detection systems (IDS) and/or intrusion prevention systems (IPS) shall be used to detect and/or prevent intrusions into the network. All IPS and IPS engines, baselines, and signatures shall be kept up-to-date.
- Malware – security systems must be in place to protect systems against computer "Malware". Refer to the Anti-Malware Policy for more information.
- Monitoring – systems shall monitor all traffic at the perimeter of environments containing sensitive information as well as at critical points in the environment containing sensitive information. Such monitoring systems shall issue alerts to personnel of any suspected compromises.
- Security structure – the security support structure shall maintain a domain for its own execution that protects it from external interference and tampering (e.g. by reading or modifying its code and data structures).
- Services – automated port scans shall be performed on a regular basis against all systems. Alerts shall be issued if unauthorized ports are detected on a system.
- Software – installing unapproved software can cause damage, invalidate warranties, or have other negative consequences. Refer to the Approved Application Policy and the Software Licensing Policy for more information.
- Timeliness – Staff shall act in a timely, coordinated manner to prevent and to respond to breaches of security to help prevent damage. However, if action is taken, it should not jeopardize the security of systems. Refer to the Incident Response Policy for more information.
- Training – F2OnSite must establish a computer security awareness and training program. Such a program requires proper planning, implementing, maintaining, and periodic evaluation. Refer to the Security Awareness and Training Policy for more information.
- User interfaces – access to specific functions shall be restricted, never allowing users to request information, functions, or other resources for which they do not have access. Three major user interfaces include menus, database views, and physically constrained user interface (e.g. access card, key, etc.).

Physical security protection

- Environmental conditions – Staff shall minimize costly disruptions caused by data or hardware loss. Refer to the Physical Security Policy to reduce risks related to environmental threats and hazards and opportunities for unauthorized access.
- Display – Staff must be aware of the visibility of data on their computer or handheld device display screens. Staff may need to reposition equipment or furniture to eliminate over-the-shoulder viewing.

For shared environments (multiple entities) the MGMT shall:

- Ensure mechanisms protect each entity's environment and data.
- Ensure that each entity only runs processes that have access to that entity's data environment.
- Restrict each entity's access and privileges to its own data environment.
- Ensure logging and audit trails are enabled and are unique to each entity's environment.
- Enable processes that provide for timely forensic investigation in the event of a compromise to any entity.

E. Incident Response Handling

F2OnSite shall establish and maintain a coordination of F2OnSite's response to computerized and electronic communication systems incidents to enable quicker remediation, information gathering and reporting of infrastructure and security related events. Refer to the Incident Response Policy for more information.

F. Emergencies and Disasters

Business continuity planning involves arranging for emergency operations of critical business functions and for resource recovery planning of these functions following a natural or man-made disruption. Refer to the Business Continuity Plan for more information.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

SECURING SENSITIVE INFORMATION POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

F2OnSite has a responsibility to maintain high standards of security for private/non-public electronic information. F2OnSite data that is stored on or accessed by computers and other electronic devices must be secured against intentional or unintentional loss of confidentiality, integrity, or availability regardless of location.

II. Purpose

This policy protects F2OnSite's assets and helps ensure our ability to continue business operations.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Computers and other devices must have an identified local Data Owner who is responsible for the data and can act as a point of contact.

Computers and other devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures by a full-time information technology professional, such as competent local IT support staff. These reviews must include adherence to baseline security requirements as well as additional strategies for protecting the information.

Units are responsible to have appropriately supervised professional technical support staffing sufficient to maintain information security. The staffing level should be appropriate to the environment considering the amount and type of private information for which they are responsible and the level of risk. Refer to the Staffing Policy for more information.

Computers and other devices must be set up in accordance with applicable F2OnSite security guidelines and standards. As received from the vendor, computers and other devices are not configured for security and require initial as well as ongoing review of the configuration and security of the operating system and software.

Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance must be performed to protect private data (Patch Management Policy). Automatic settings or centralized updating of security patches is recommended for most desktop computers.

Access to private data must be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator or root level passwords should be exceptionally strong, since these accounts allow complete control of the system. User accounts with fewer privileges should be used instead of root accounts whenever possible. Periodic review of access is required.

If sent across the Internet (external to the F2OnSite's network) or other open networks such as wireless connections, both the authentication data (e.g. user ID and password) and the data itself must be encrypted with strong encryption. Encryption of private data stored on laptop computers or other portable devices is required. An off-site plain-text backup version in a secure location is recommended to protect against lost encryption keys. The F2OnSite's wired network is not considered an open network.

Desktop and laptop computers must have anti-virus software or filters installed and updated daily (automatic updates recommended). In addition, other Windows computers, including servers, must have anti-virus software installed and updated daily. (See the Anti-Malware Policy).

Physical access to computers must be restricted as much as possible. Devices not in use for extended periods (e.g. at night and on weekends) must be turned off. Laptops must be physically restrained (e.g. via an anchoring device) at work stations and servers must be in an appropriate and secure physical facility.

Password protected screen saver programs should be used in open locations. Password protected screen savers are required and should be set per the Securing Information Systems Policy.

Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs). Refer to the Logging Policy for additional information on log files.

Servers storing private data must be scanned regularly with vulnerability testing software so that corrective actions can be taken as appropriate. Desktop vulnerability

scans are regularly sent to the IT technical support staff for review. Servers storing private data are scanned regularly with vulnerability testing software with corrective actions taken as appropriate.

Sensitive Information in databases, logs, data files, backup media, etc. shall be stored securely by means of encryption, masking, truncation, etc. Refer to the Encryption Policy for more information.

Periodic backup copies of software and data must be made, tested, and stored securely. The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems. Refer to the Backup Policy for more information.

A "secure deletion" program must be used to erase data from hard disks and media prior to transfer or disposal of hardware. Permanent media (e.g., CD's, DVD's, etc) must be physically destroyed. Refer to the Disposal Policy for more information.

Services available on computers or other devices must be as limited as much as possible. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to private data. Unless a high level of expertise is available and these services are closely monitored at all times, this higher risk software should not be installed.

Training provided by F2OnSite on data security practices must be completed for both new and existing employees. Employees that deal with sensitive data may require additional training. Refer to the Security Training Policy for more information.

One or more of the following additional actions should be used to further protect Sensitive Information, depending upon the situation and requirements:

- Limit storage of private data to a hardened file server at the department level.
- Severely restrict the volume and duration of the information stored.
- Move the data to a dedicated computer holding no other applications or data.
- Limit network access to a list of specific machines or devices (access control list).
- Use an internal F2OnSite, non-routed IP address or network which prevents any access either to or from the Internet
- Encrypt stored data (with a clear-text version on a removable medium stored in a safe location).
- Sign up for notification of security patch availability from vendors
- Separate any sensitive data from other data and store independently (e.g. on a non-networked device).

F2OnSite departments must conduct periodic reviews of information systems in their control that contain private or confidential data.

Each department is required to document the activities they will conduct to review information systems activity. These activities must include:

- Regular review of list of users who have been granted access to systems that contain protected or private information to ensure that only those who need access have access to the systems.
- Periodic review of departmental or unit data security incident trends.
- Periodic review of departmental or unit policies and practices to ensure they address emerging data security trends in the department.
- Document the completion of the periodic reviews described above.
- Periodic review of audit logs.
- Periodic review of user areas to ensure a clear desk for papers and removable storage media and a clear screen. See the Clear Desk Policy for more information.

IT Systems Administrators have the following responsibilities:

- Establish and publish the criteria upon which a server is determined to be a "critical server".
- Periodically review critical server list based on established criteria.
- Perform and review vulnerability scans of critical servers.
- Implement intrusion detection system and review.
- Perform and review ad hoc scans for emerging threats.
- Monitor local data security compliance in the areas for which they are responsible.

A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to protect against Internet threats and to limit network access to devices storing Sensitive Information. Refer to the Firewall Policy for more information.

- Firewalls shall be installed at each Internet connection and between any demilitarized zone (DMZ) and the internal network.
- Firewalls shall be installed and active on mobile devices such as Laptops and similar devices.
- Inbound Internet traffic shall be limited to IP addresses within the DMZ. Firewalls shall not allow direct traffic between the Internet and sensitive data.

Documentation shall be maintained per the Documentation Policy. Firewall documentation shall include:

- Services and ports allowed (inbound and outbound)
- Business need for each service and port

- Information security features to be implemented
- Date of last change

The Chief Security Officer (MGMT) shall ensure policies and procedures govern the collection, use, processing, storing, transmitting, and disclosing of Sensitive Information.

- Policies and procedures are clear, reasonable, and protect Sensitive Information.
- Consent is obtained before collecting, using, and disclosing Sensitive Information.
- Sensitive Information is collected in reasonable, appropriate, and lawful ways.

The MGMT shall ensure Sensitive Information is:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than necessary.
- Processed in accordance with the data's rights.
- Secure.
- Transferred only to areas with adequate protection.

The MGMT shall ensure that data is classified per the Data Classification Policy. Data shall be properly protected according to its classification. Specific security requirements can include:

- Access Controls – see the Access Control Policy
- Awareness and Training – see the Security Awareness and Training Policy and Security Awareness and Training Plan
- Audit and Accountability – see the Audit Policy and Audit Trails Policy
- Configuration Management – see the Security Information Systems Policy, Firewall Policy, Server Hardening Policy, and Router Security Policy
- Identification and Authentication – see the Logical Access Controls Policy
- Incident Response – see the Intrusion Detection Policy, Incident Response Policy, and Incident Response Plan
- Maintenance – see the IT Management Policy
- Media Protection – see the Removable Media Policy and the IT Management Policy
- Personnel Security – see the Personnel Security Policy
- Physical Protection – see the Physical Security Policy and Physical Access Policy
- Risk Assessment – see the Risk Assessment Policy and Risk Management Policy
- Security Audit – see the Security Controls Review Policy, Audit Policy, Audit Trails Policy, and Logging Policy

- System and Communications Protection – see the Security Policy
- System and Information Integrity - see the Audit Trails Policy, Logging Policy, Patch Management Policy, Anti-Malware Policy, Security Policy, and Intrusion Detection Policy

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff that use F2OnSite Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.02, APO01.11, APO13.07, APO14.01-02, APO14.07, APO14.10, MEA03.01
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5, A.7.2.2, .A8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8

SECURITY AWARENESS AND TRAINING PLAN

I. Purpose of the Security Awareness and Training Plan

F2OnSite understands that "people", not technology vulnerabilities, can be the biggest threat to our Information Resources. The purpose of this Security Awareness and Training Plan (Plan) is to ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.

II. Overview of the Security Awareness and Training Plan

A strong security program requires Staff to be trained on security policies, procedures, and technical security controls. F2OnSite Staff who manage Information Resources need to have the necessary skills to carry out their assigned duties.

The Chief Security Officer (MGMT) is responsible for developing, implementing, and maintaining this Plan. This Plan documents the process for Staff security training, education, and awareness and ensures that F2OnSite Staff understands its role in protecting the confidentiality, integrity, and availability of Information Resources.

This Plan ensures that Staff is provided with regular training, reference materials, and reminders to enable them to appropriately protect F2OnSite's Information Resources. Training shall include, but is not limited to:

- F2OnSite's responsibilities for protecting Information Resources.
- Risks to Information Resources.
- The secure use of Information Resources.
- Information security policies, procedures, and best practices.

This Plan ensures:

- All new users attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any IT resources.
- Staff receives training appropriate for specific job roles and responsibilities. After training, each Staff member verifies that he or she received the training, understood the material presented, and agrees to comply with it.
- Staff is trained on the importance of enabling and utilizing secure authentication.
- Staff is trained on how to identify, report, and prevent security incidents as well as the most common indicators of an incident.

- Staff is aware of causes for unintentional data exposures, such as losing their mobile devices or e-mailing the wrong person due to autocomplete in e-mail.
- Staff is trained on how to identify and properly store, transfer, archive, and destroy sensitive information.
- Security policies, procedures, and manuals are readily available for reference and review by the appropriate Staff.
- Staff attends annual security awareness training sessions.

III. Security Awareness and Training Lifecycle

F2OnSite cannot protect the confidentiality, integrity, and availability of information without ensuring that all Staff involved in using and managing Information Resources:

- Understand their roles and responsibilities.
- Understand F2OnSite's security policies and procedures.
- Have at least adequate knowledge of the various administrative, physical, and technical controls to protect the Information Resources for which they are responsible.

The MGMT ensures that F2OnSite Staff understands the concepts and strategy of the organization's security awareness and training program. Security begins with awareness, builds to training, and evolves into education.

- *Awareness.* Security awareness efforts change behavior or reinforce good security practices. Awareness is not training. The purpose of awareness is to focus attention on security. Awareness presentations help individuals identify security issues and the proper response to security threats.
- *Training.* While security awareness relies on reaching broad audiences with attractive presentations, training tends to be more formal, with a goal of building knowledge and skills that enhance the effectiveness of security controls. Training strives to produce relevant and needed security skills and competencies by F2OnSite Staff.
- *Education.* Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adding concepts, issues, and principles to produce security specialists and professionals capable of pro-active response to threats.

F2OnSite's security awareness and training program lifecycle consists of the following elements:

1. Designing the Security Awareness and Training Program – an assessment is conducted and a training strategy is developed and approved. This strategic planning process identifies implementation tasks to be performed in support of security training goals.
2. Developing Material for the Security Awareness and Training Program – available training resources are identified as is the scope and content of the training material.

3. Implementing the Security Awareness and Training Program – effective communication and roll out of the awareness and training program including options for delivery of awareness and training material (e.g. web-based, distance learning, video, and on-site).
4. Security Awareness and Training Post-Implementation – guidance on keeping the program current and monitoring its effectiveness including the use of feedback methods (e.g surveys, focus groups, and benchmarking).

IV. Designing the Security Awareness and Training Program

The awareness and training program helps to support the business needs of the organization. The responsibility and budget for F2OnSite’s security awareness and training program is developed, managed, and maintained by the MGMT. All directives, strategy development, planning, and scheduling is coordinated through this “security awareness and training” authority.

The MGMT communicates to F2OnSite’s departments the policy directives regarding security awareness and training, the strategy for conducting the program, and the material and methods of implementation. The Department Heads then provide information requested by the MGMT.

The MGMT collects data on the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. Department Heads provide feedback on the effectiveness of awareness and training material and on the appropriateness of the methods used to implement the material. Department Head feedback allows the MGMT to fine-tune, add or delete material, or modify the implementation methods.

On an annual basis, the MGMT conducts a needs assessment that reviews and determines F2OnSite’s awareness and training needs. The needs assessment supports management’s decision to allocate adequate resources to meet the identified awareness and training requirements and considers various types of Staff:

- Executive Management – management understands directives and laws that form the basis for the security program. They also understand leadership roles to ensure full compliance by users.
- Security Personnel – security program managers and security officers act as expert consultants and are well educated on security policies and security best practices.
- System Owners – system and data owners have an understanding of security policies and a high degree of understanding security controls and requirements applicable to the systems they manage.

- System Administrators – administrators are critical to a successful information security management system and have a higher degree of security technical knowledge and training.
- Operational Managers and System Users – managers and system users have a high degree of security awareness and training on security controls and rules of behavior for systems they use and manage.

Methods to collect information for the needs assessment include:

- Interview or survey of IT department, system and data owners, and key Staff.
- Review and assessment of available resource material (e.g. current awareness and training materials, training schedules, and lists of attendees).
- Analysis of metrics related to awareness and training (e.g., percentage of Staff completing required awareness session or exposure, percentage of Staff who have significant security responsibilities who have been trained in specific material).
- Review of security plans for general support systems and major applications to identify system and application owners and appointed security representatives.
- Review of application user IDs to identify Staff who have access to Information Resources.
- Review of audit findings and/or recommendations related to the security of Information Resources.
- Analysis of events (e.g. denial of service attacks, virus damage, Ransomware, and website defacements).
- Security trends and metrics.

Metrics are an important tool used to help determine the effectiveness of F2OnSite's security awareness and training program. Metrics monitor the program goals and objectives by:

- Quantifying the level of program implementation.
- Identifying the effectiveness and efficiency of the program.
- Analyzing the adequacy of awareness and training efforts
- Identifying possible improvements.

The needs assessment identifies:

- The awareness, training, and/or education needs of the organization.
- Tasks currently performed to address the above needs.
- How the training needs are being addressed and the effectiveness of the training.
- Training "gaps" between the needs of the organization and what is currently being provided.
- A prioritized list of critical needs.

The MGMT analyzes the needs assessment and develops an awareness and training strategy. The strategy identifies:

- The personnel responsible for designing, developing, implementing, and maintaining the security awareness and training material.
- The personnel responsible for ensuring that the appropriate Staff attend or view the applicable material.
- The goals to be accomplished for each aspect of the program (e.g., awareness, training, education).
- Target audiences for each aspect of the program. Mandatory and optional courses or material for each target audience.
- Learning objectives for each aspect of the program. Topics to be addressed in each session or course.
- Deployment methods to be used for each aspect of the program.
- Documentation, feedback, and evidence of learning for each aspect of the program.
- Processes to evaluate and update the security awareness and training material.
- The frequency that each target audience should be exposed to material.

Once the security awareness and training strategy has been finalized, the MGMT develops a prioritized implementation schedule. Key factors to consider include:

- Availability of materials and resources.
- Role and impact on the organization.
- Current situation and “gaps” from needs assessment.
- Critical project dependencies.

V. Developing Material for the Security Awareness and Training Program

The secure awareness and training material identifies the behavior to be reinforced (awareness). Since the goal of awareness is to focus attention on good security practices, the message is short and simple. The awareness audience includes all users and makes them aware of commonly shared security responsibilities.

Training material identifies the skills the audience should learn and apply. A typical training class is directed at a specific audience and emphasizes what attendees need to know in order to do their jobs. Training material is usually far more in-depth than material used in awareness sessions.

Security awareness topics include:

- Acceptable use and monitoring of user activity
- Access controls, least privilege, and separation of duties
- Bring your own device and technology (BYODT)

- Change management
- Data backup and storage
- Desktop security (e.g. screen savers, time outs)
- E-mail, spam, and attachments
- Encryption and transmitting sensitive information
- Equipment disposal
- Handheld (mobile) devices
- Incident response contacts
- Laptop security
- Malware, viruses, worms, and Ransomware
- Password usage and management
- Patch management
- Physical access
- Security policies and implications of non-compliance
- Shoulder surfing
- Social engineering attacks including phishing, phone scams and impersonation calls
- Software license restrictions
- Supported software

Security awareness material includes both a single theme (e.g. posters) as well as combining a number of themes or messages into a presentation. Sources of material on security awareness include:

- Conferences, seminars, and courses.
- E-mail advisories issued by industry sources.
- Professional organizations and vendors.
- Security magazines and periodicals.
- Security news websites.

The MGMT shall identify Staff members who require special security training:

- Acquire. Staff who acquire Information Resources.
- Administrator. Staff who operate (administer) Information Resources.
- Design and Develop. Staff who program, design, and develop systems and applications.
- Manage. Staff who manage Information Resources.
- Review and Evaluate. Staff who review and evaluate (audit) Information Resources.

The MGMT determines if training materials will be developed in-house or through the use of outside services. Key factors considered when determining if the material will be developed in-house vs. outsourced include:

- In-house resources, knowledge, and experience to prepare the material.
- Cost of developing the material vs. packaged materials.
- Course content sensitivity.

- Material delivery schedules.

VI. Implementing a Security Awareness and Training Program

F2OnSite's security awareness and training program includes a needs assessment and gap analysis, a formal program strategy, a plan to prepare program materials, and a plan to implement the strategy.

Communications with management and Staff is an essential part of implementing the program to ensure active support and commitment of necessary resources. The MGMT:

- Documents the expected results of the program, anticipated costs, and benefits to the organization.
- Communicates the program schedule and offerings to the organization's Department Heads.

Techniques for delivering material include:

- Computer based training
- E-mails
- Flyers
- Instructor led sessions
- Message boards
- Newsletters
- Posters
- Teleconferences
- Videos
- Webinars

Programs take advantage of technology that supports the following features:

- Ease of use and access.
- Scalability for small to large audience sizes and locations.
- Accountability and ability to track attendance and participation.

VII. Security Awareness and Training Program Post-Implementation

Once the program has been implemented, processes monitor Staff attendance and effectiveness. A tracking system captures key information and program activity (e.g., courses, dates, audience, costs, and training sources). The tracking system captures data by department so that it can be used to provide enterprise wide analysis and reporting regarding awareness, training, and education initiatives.

Compliance tracking maps program activities to standards established by the MGMT. Reports are generated and used to identify gaps or problems so that the appropriate corrective action can be taken.

Formal evaluation and feedback mechanisms are critical components of the security awareness, training, and education program. Continuous improvement and feedback processes ensure the program is working as desired.

Feedback mechanisms include:

- Evaluation forms and questionnaires.
- Focus groups.
- Formal status reports.
- Independent observation and analysis.
- Security program benchmarking (external view).
- Selective Interviews.

The MGMT and Department Heads are the primary advocates for continuous improvement and support of F2OnSite's security awareness, training, and education program. Listed below are key indicators that gauge the support for, and acceptance of, the program:

- Sufficient funding by F2OnSite senior management.
- Support for broad distribution and posting of security awareness items.
- Senior management messages to staff regarding security.
- Use of metrics to identify security trends.
- Managers do not use their position to avoid security controls.
- Required attendance at security awareness and training sessions.
- Recognition of security contributions through awards and contests.

Corrective action is taken and includes formal reminders, additional awareness, training, or education offerings, and external social engineering evaluations by independent auditors.

Appendix A – Distribution List

President

Chief Operating Officer

IT Director

All Department Heads

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) Security Awareness and Training Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

SECURITY AWARENESS AND TRAINING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

People, not technology vulnerabilities, can be the biggest threat to our Information Resources. Staff must receive security awareness and education training appropriate for their job duties and responsibilities.

II. Purpose

A strong security program requires Staff to be trained on security policies, procedures, and technical security controls. F2OnSite Staff who manage Information Resources need to have the necessary skills to carry out their assigned duties. The purpose of this Security Awareness and Training Policy is to ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.

III. Scope

This policy applies to all F2OnSite Staff who use Information Resources.

IV. Policy

F2OnSite management must ensure that high priority is given to effective security awareness and training. This includes implementing a viable security program with a strong awareness and training component. F2OnSite management shall designate a Chief Security Officer (MGMT) responsible for the security of Information Resources. The MGMT shall ensure that a well-supported (e.g. resources and budget) and effective security program is implemented and maintained.

F2OnSite's MGMT shall be responsible for developing, implementing, and maintaining a Security Awareness and Training Plan (Plan). This Plan shall document the process for Staff security training, education, and awareness and ensure that F2OnSite Staff understand their role and responsibility in protecting the confidentiality, integrity, and

availability of Information Resources. Communications relevant to the information security management system (ISMS) include what to communicate, when to communicate, with whom to communicate, who shall communicate, and the process by which communication shall be affected. Communications shall be issued in a continuous and engaging manner.

The Plan shall ensure that Staff is provided with regular training, reference materials, and reminders to enable them to appropriately protect F2OnSite's Information Resources. Training shall include, but is not limited to:

- F2OnSite's responsibilities for protecting Information Resources
- Risks to Information Resources
- How to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls
- The secure use of Information Resources
- Information security policies, procedures, and best practices

The Plan shall ensure:

- All new users attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Information Resources.
- Staff receives training appropriate for specific job roles and responsibilities. After such training, each Staff member must verify that he or she received the training, understood the material presented, and agrees to comply with it.
- Staff are trained on how to identify, report, and prevent security incidents. Staff are aware of the most common indicators of an incident.
- Staff understand the importance of enabling and utilizing secure authentication.
- Staff identify and properly store, transfer, archive, and destroy sensitive information.
- Security policies, procedures, and manuals are readily available for reference and review by the appropriate Staff.
- Staff attend annual security awareness training.
- Staff sign an acknowledgement stating they have read and understand Pacific Steel & Recycling requirements regarding computer and information security policies and procedures.
- Staff are provided with sufficient training and supporting reference materials to allow them to properly protect Pacific Steel & Recycling's Information Resources.
- The IT Department prepares, maintains, and distributes one or more information security manuals that concisely describe information security policies and procedures.

- Cloud computing security awareness training programs address multi-tenant, nationality, and cloud delivery models. Conflicts of interest shall be established for all Staff and Tenants.
- Staff are made aware of the risks and responsibilities related to bring your own device and technologies (BYODT).
- Staff are aware of causes of unintentional data exposures, such as losing their mobile devices or e-mailing the wrong person due to autocomplete in e-mail.

The MGMT shall:

- Ensure a skills gap analysis is performed to understand the skills and behaviors Staff are not adhering to and use of this information to build a baseline education roadmap.
- Develop and maintain a communications process to communicate new security program, security bulletin, and security items of interest.
- Ensure that Staff responsible for implementing Information Resources safeguards receives formal training in security best practices.
- Ensure periodic security reminders (flyers or posters, e-mails, verbal updates at meetings) keep Staff up-to-date on new and emerging threats and security best practices. The frequency and method of delivery of such reminders shall be determined by the MGMT.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	06/30/2020	Updated Initial policy release	D LAUDERBACK

References:

COBIT EDM01.03, APO02.08, APO07.12-13, APO12.02, APO12.07, APO13.07,
MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(D)
ISO 27001:2013 7.2(b), 7.3, A.7.2.2, A.12.2.1
NIST SP 800-37 3.3, 3.4, 3.5, 3.7
NIST SP 800-53 AT-2, AT-3, CP-3, IR-2, PM-13, SI-3, SI-4(24)
NIST Cybersecurity Framework DE.DP-1, ID.GV-1, PR.AT-1-5, RS.RP-1, RS.MI-2
PCI 6.5, 9.9, 12.6.1-2, 12.10.4, A3.1.4

SECURITY CONTROLS REVIEW POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Security controls and safeguards are part of F2OnSite's Risk Treatment Plan to mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

Risk is the potential that a threat will exploit one or more asset vulnerabilities and result in a loss or failure to achieve an objective. At F2OnSite, risk management is the process of identifying, analyzing, and the use of safeguards and controls to treat risks. This policy establishes a formal and periodic review of security control and safeguards.

III. Scope

This policy applies to the Risk Management Officer and F2OnSite Department Heads.

IV. Policy

F2OnSite's Risk Management Officer shall be responsible for reviewing safeguards and controls on an annual basis. The purpose of the review will be to ensure the controls are sufficient, appropriate, and effective at managing and reducing risks to acceptable levels.

Per the Risk Management Policy, on an annual basis each F2OnSite Department Head will prepare and provide to the Risk Management Officer, a Risk Assessment, Risk Analysis, and a Risk Treatment Plan. Collectively, these documents specify specific security controls and safeguards.

The Risk Management Officer will review the security controls to ensure they are aligned with the needs of the organization. The Risk Management Officer may choose to have security controls independently reviewed by a Certified Information Systems

Auditor (certified by the Information Systems Audit and Control Association) to ensure they are sufficient, appropriate, and effective at managing and reducing risks.

As necessary, the Risk Management Officer will recommend to the appropriate Department Heads changes or enhancements to security controls and safeguards. This process helps ensure each department's approach to managing risk is properly aligned with the needs of the organization.

Security controls can be classified according to their approach to security incidents:

- Preventive controls – These safeguards prevent security incidents. Examples include passwords, encrypting laptop hard drives, cards that permit physical access to data centers, etc.
- Detective controls – During an event, detective controls identify and characterize an incident in progress. Examples include anti-virus software, alarms and notifications, etc.
- Corrective controls – Limit the extent of damage caused by the incident and assist in resuming normal business operations.

Security controls may also be classified according to their nature, for example:

- Administrative controls – Safeguards include formal and informal policies, procedures, and security training.
- Physical controls – Protection mechanisms that protect physical assets (e.g. access cards, data center server racks, locking cabinets).
- Technical controls – Technical safeguards (e.g. logical access controls, passwords, patch management, security assessments)

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite Executive Management, Department Heads, IT Director, Risk Management Officer, and Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	UPDATED Initial policy release	D LAUDERBACK

References:

COBIT APO01.11, APO03.06, APO11.09, APO12.02, APO12.07, DSS05.07, MEA04.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(i), 164.308(a)(8), 164.308(a)(2)
ISO 27001:2013 9.3, A.5.1.2, A.9.1.1, A.18.2
NIST SP 800-37 3.5, 3.7
NIST SP 800-53 All XX-1 controls, CA-2, CA-7
NIST Cybersecurity Framework ID.RM-1, PR.PT-1, DE.CM-8, DE.DP-5
PCI 6.7, 7.3, 8.1, 8.8, 12.5, 12.8

SECURITY MONITORING POLICY

Policy Area	IT Policy Library
Approved Date	July 1, 2020
Approved By	Policy Committee
Effective Date	July 2, 2020
Current Version	2.1

I. Overview

Security monitoring confirms that F2OnSite's security mechanisms and controls are in place, are effective, and are not being bypassed.

II. Purpose

One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning.

III. Scope

This policy applies to all Staff responsible for the installation of new IT resources, the operations of existing resources, and charged with IT security.

IV. Policy

Automated tools provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline shall be developed and tools used to report exceptions. Tools shall be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Operating system security parameters

The following files shall be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by the Risk Management Officer:

- Automated intrusion detection system logs

- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Help desk trouble tickets
- Telephone activity (e.g. call detail reports)
- Network printer and fax logs

A evaluation of Information Systems by IT security Staff shall be performed on an annual or more frequent basis as needed. Such evaluations shall include a review of:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Unauthorized remote connectivity
- Unauthorized operating systems
- Unauthorized software licenses

Any security issues discovered will be reported to the IT Director for follow-up investigation.

Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) shall monitor network traffic and alert personnel to suspected compromises. IDS and IPS systems shall be maintained and kept up-to-date. Any changes shall be authorized by the appropriate asset Owner and logged. IDS and IPS systems shall be updated in a timely manner with vendor supplied patches. IDS/IPS detection alerts shall be issued if suspected intrusions or other unauthorized activities have occurred.

Procedures shall be developed to monitor and record growth and traffic patterns, bandwidth issues, etc. Appropriate reporting shall be in place to allow IT to anticipate performance issues and delays and react in a timely and proactive manner.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite Executive Management, Department Heads, IT Director, Risk Management Officer, and Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D. Lauderback

References:

COBIT EDM03.07, APO01.11, APO09.05, APO13.07, DSS01.05, DSS05.02, DSS05.07
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(C), 164.312(b)
ISO 27001:2013 9.1, 9.3, A.12.1.3, A.12.4, A.15.2.1
NIST SP 800-37 3.7
NIST SP 800-53 AU-3-4, AU-5(1), AU-6, AU-11-12, AU-14, CP-2(2), SA-9 SC-5(2)
NIST Cybersecurity Framework PR.AC-1-2, PR.AC-4, PR.PT-1, DE.AE-1-5, DE.CM-1-7
PCI 8.1.5, 9.1, 10.2, 10.4.2.b, 10.5.5, 10.6-7

SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Security systems and processes help protect F2OnSite's Information Resources and ensure system confidentiality, availability, and integrity.

II. Purpose

This policy identifies security safeguards and controls that help F2OnSite manage risks, meet business requirements, and comply with regulations.

III. Scope

This policy applies to all Staff that use F2OnSite's Information Resources.

IV. Policy

A. Security Overview

THE MGMT SHALL ENSURE SECURITY SAFEGUARDS AND CONTROLS ARE IMPLEMENTED AND MAINTAINED TO ACHIEVE THE DESIRED SECURITY OBJECTIVES:

- Availability. Information Resources are available and operational when and where they are needed.
- Confidentiality. Only authorized individuals have access to information.
- Integrity. The value and state of information is protected from unauthorized modification.

THE CHIEF SECURITY OFFICER (MGMT) IS RESPONSIBLE FOR IMPLEMENTING AND MAINTAINING:

- ADMINISTRATIVE SAFEGUARDS
- TECHNICAL SAFEGUARDS
- PHYSICAL SAFEGUARDS

B. Administrative Safeguards

Administrative safeguards provide top down security direction and guidance. Administrative safeguards are written documents grouped into major categories.

Confidentiality. The requirements for non-disclosure (e.g. confidentiality agreements) reflect F2OnSite's need for to protect data and operational details. Such requirements shall be identified, documented, and reviewed at planned intervals.

Data Owners. The roles and responsibilities of the Data Owners and department head custodians shall be formally defined. Equipment and data shall not be taken off-premise without prior approval from the Data Owner.

Independent Reviews (Audits). Where possible, the MGMT shall use Certified Information Systems Auditors, or equivalent, to audit the security controls of F2OnSite's Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources. Refer to F2OnSite's Audit Policy for more information.

Insurance. Property and cyber insurance can be used to transfer risk. The MGMT shall work with the Risk Management Officer (RMO) to determine required coverages.

Job descriptions. Executive Management shall ensure job descriptions exist for all employees. Each job description shall identify the position title, purpose of the position, specific duties and responsibilities, reporting relationships, position requirements, and related information.

Plans. Written plans shall be developed and maintained to ensure safeguards controls business risks. Important plans include:

- **Business Continuity Plan.** The purpose of this plan is to protect Information Resources and our ability to continue business operations in the event of a disaster or component failure. For more information see the Business Continuity Plan.
- **Incident Response Plan.** The Incident Response Plan helps protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. Staff shall act in a timely and coordinated manner prevent and to respond to breaches of security to help prevent damage. However, if action is taken, it should not jeopardize the security of systems. Refer to the Incident Response Policy and Incident Response Plan for more information.
- **Security Awareness and Training Plan.** The Security Awareness and Training Plan help ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.
- **System Security Plan.** The System Security Plan (Plan) shall provide an overview of the security requirements of Information Resources. This Plan also describes the controls necessary to ensure information availability, confidentiality, and integrity.

Policies. THE CHIEF SECURITY OFFICER (MGMT) SHALL BE RESPONSIBLE FOR IMPLEMENTING AND MAINTAINING SECURITY POLICIES, PROCEDURES, PLANS, FORMS, AND RELATED DOCUMENTS.

- Account management. Policies and procedures shall manage the process of creating, monitoring, controlling, and removing of accounts. Refer to the Account Management Policy for more information.
- Classification. All users, hosts, and data shall be classified per the Data Classification Policy.
- Logging. Host security log files shall be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs). Refer to the Logging Policy for more information.
- **UPDATES. ON AN ANNUAL BASIS, OR MORE FREQUENTLY IF NEEDED, POLICIES, PROCEDURES, PLANS, FORMS, ETC. SHALL BE REVIEWED AND UPDATED BY THE MGMT TO ADDRESS ORGANIZATIONAL CHANGES AND ENSURE CONTINUAL IMPROVEMENTS IN THE INFORMATION SECURITY MANAGEMENT SYSTEM. ANY NEW DOCUMENTS, OR UPDATES TO EXISTING DOCUMENTS, SHALL BE APPROVED BY EXECUTIVE MANAGEMENT PRIOR TO BEING DISTRIBUTED TO F2ONSITE STAFF.**
- Use. Users are a first line of defense and shall follow safe computing practices as outlined in the Acceptable Use Policy.

Risk Assessment. Risk assessments help identify business processes that are of high priority and importance to the organization. They also ensure the proper controls are implemented to reduce risks to acceptable levels. The risk assessment and risk analysis shall identify threats including the likelihood of the event and impact on the organization. Preventive, detective, and corrective controls shall be identified and implemented as needed. For more information see the Risk Assessment Policy.

Staffing. All departments shall have appropriately supervised staff sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of information for which they are responsible and the level of risk.

C. Technical Safeguards

Technical safeguards protect and control access to Information Resources.

Access Controls.

- Authentication data. Information Systems shall protect authentication data as it is entered including suppressing the display of the password as it is entered, and orienting keyboards away from view.
- Inactive IDs. User IDs that are inactive on the system for a period of three months shall be deleted.
- Inactivity – users shall be automatically logged off after 15 minutes of inactivity.
- Logon attempts – users shall be locked out after five consecutive failed logon attempts within a 24 hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID.

- Passwords – passwords are a key component to system security and restricting access to systems. Refer to the Password Policy for more information.
- Screen savers - protected screen savers are required and shall be activated after 15 minutes of inactivity.
- User interfaces. Access to specific functions shall be restricted, never allowing users to request information, functions, or other resources for which they do not have access. Three major user interfaces include menus, database views, and physically constrained user interface (e.g. access card, key, etc.).

Clear desk. Staff shall ensure sensitive information remains secure by clearing their desks when they will be away from their office, positioning monitors to prohibit unauthorized viewing, etc. See the Clear Desk Policy for more information.

Communications

- Border routers. Border routers may be used to filter traffic and protect against spoofed IP addresses.
- Firewalls. Firewalls shall protect the network and limit traffic to only approved activities. For more information see the Firewall Policy.
- Transaction. Transaction based access criteria can be used. For example, access to a particular account could be granted only for the duration of a transaction. When completed, the access authorization is terminated.

Data handling. Controls and safeguards shall be implemented to protect the integrity of electronic data that is stored, accessed, or transmitted. Refer to the Data Integrity Policy.

Lifecycle. The MGMT shall ensure that information is protected during its entire lifecycle. Information shall only be retained for the duration of its useful life. The disposal of hardware, software, and information requires special consideration. Refer to the Data Retention Policy, Disposal Policy, Encryption Policy, and Removable Media Policy for more information. F2OnSite's IT Department shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). Please refer to the Software Development Policy for more information.

Monitoring. Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing F2OnSite's Information Resources. Audit trails can also be used as an incident detection and response mechanism. Refer to the Audit Trails Policy and Logging Policy for more information.

Network management

- Backups. Backups shall be protected against accidental or deliberate destruction of data. Refer to the Backup Policy for more information.
- Configurations. Information Systems shall be configured according to applicable security guidelines and standards. As received from the vendor, computers and other devices may not be configured for security and may require initial as well as ongoing review of the configuration and security of the operating system and software. Staff must protect data by implementing and maintaining authorized hardware and software configurations. Network administrators shall implement and maintain documented security configuration standards for all authorized operating systems and software. Network administrators shall use a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. For more information see the Network Configuration Policy, Server Hardening Policy, and Workstation Security Policy for more information.
- Management. Networks shall be managed and controlled to protect information in systems and applications. The network and security architecture, including data flow diagrams, shall be documented and aligned with industry best practice standards. For more information see the Configuration Management Policy and Network Security Policy.
- Service levels. Service levels and management requirements of all network and security services shall be identified, documented, and agreed upon by Data Owners and IT Staff. Service levels and requirements shall be included in appropriate third-party service level agreements (SLA). Metric based performance shall be reported according to agreed upon schedules.
- Segments. Network equipment (e.g. routers, servers, workstations) shall be classified and placed in a network segment appropriate to its level of classification. Access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification then the data shall be protected in a manner appropriate to its classification level. Groups of information services, users, and information systems shall be segregated on networks. IT security Staff shall consider the use of ACLs and Virtual Local Area Networks (VLANs) to segment systems and enhance security. ACLs are a register of users (e.g. groups, machines, processes) permitted to use a particular system resource and the types of access they have been permitted.

Security protection

- **Change.** Every change to an Information Resource (e.g. operating system, computing hardware, networks, applications, data centers) is subject to the Change Management Policy and must follow appropriate change management procedures. Where appropriate, change detection systems (e.g. file-integrity monitoring tools) shall alert personnel to unauthorized modification of critical system files, configuration files, or content files. Such systems shall be configured to perform critical file comparisons at least weekly. Note: For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by IT security Staff. IT security Staff shall implement a process to respond to any alerts generated by the change detection solution.
- **Encryption.** Systems and media may contain Sensitive Information. Refer to the Encryption Policy for more information on restricting access to Sensitive Information.
- **Forensic investigations.** Processes shall provide for timely forensic investigation in the event of an incident.
- **Intrusions.** Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) shall be used to detect and/or prevent intrusions into the network. All IPS engines, baselines, and signatures shall be kept up-to-date.
- **Malware.** Security systems shall be in place to protect systems against computer malicious software. Refer to the Anti-Malware Policy for more information.
- **Software.** Installing unapproved software can cause damage, invalidate warranties, or have other negative consequences. Refer to the Approved Application Policy and the Software Licensing Policy for more information.
- **Patching.** Information Systems shall be patched and updated in a timely manner. See the Patch Management Policy for more information.
- **Monitoring.** Systems shall monitor all traffic at the perimeter of environments containing Sensitive Information as well as at critical points in the environment containing Sensitive Information. Such monitoring systems shall issue alerts to personnel of any suspected compromises.
- **Shared environments.** For multiple entity shared environments the MGMT shall ensure mechanisms protect each entity's environment and data. Each entity only runs processes that have access to that entity's data environment. Each entity's access and privileges shall be restricted to its own data environment. Logging and audit trails shall be enabled and unique to each entity's environment.

Third party access. Prior to granting individuals physical or logical access to information resources, agreements with staff, third party users, and customers shall be in place and

include responsibility for information security. Refer to the Third Party Service Providers Policy for more information.

D. Physical Safeguards

Physical safeguards include mechanisms that protect physical assets (e.g. access cards, data center server racks, locking cabinets, cameras, uninterruptable power, guards, etc.). Physical safeguards shall ensure only authorized Staff have access to Information Systems, equipment, and operating environments. For more information see:

- Facility Security Plan
- Physical Access Policy
- Physical Security Policy

Media. Media shall be handled according to the Removable Media Policy.

Operations.

- Acquisitions. Only hardware or software acquired through F2OnSite's approved policies and procedures may be installed. Refer to the Acquisition and Procurement Policy.
- Diagnostic ports. Physical and logical access to diagnostic and configuration ports shall be controlled. Refer to the Network Configuration Policy and Physical Access Policy.
- Location. Access to Information Resources may be based upon physical or logical location. Similarly, users can be restricted based upon network addresses (e.g., internal users may be permitted greater access than those from outside the organization).
- Time. Time and day restrictions may be used to limit access to data (e.g. access to personnel files may only be allowed during normal working hours).

Physical security protection

- Access. Access to Information Resources shall be controlled and restricted as much as possible. Devices not in use for extended periods shall be turned off. Workstations and servers shall have appropriate and secure physical controls. Refer to the Physical Security Policy for more information.
- Display. Staff shall be made be aware of the visibility of data on their computer or handheld device display screens. Staff shall position equipment or furniture to eliminate over-the-shoulder viewing.
- Environmental conditions. Staff shall minimize costly disruptions caused by data or hardware loss. Refer to the Physical Security Policy to reduce risks related to environmental threats and hazards and opportunities for unauthorized access.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff that use F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	Donny Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5, A.7.2.2, A8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8, PCI Software Security Framework

SECURITY SELF ASSESSMENT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Security self assessments are part of F2OnSite's controls and safeguards designed to identify, mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

Security self assessments help ensure F2OnSite's security controls and safeguards adequately protect Information Resources. By knowing the current status of information systems and information security programs, F2OnSite can determine the appropriate risk treatment option.

III. Scope

This policy applies to F2OnSite Executive Management, Chief Security Officer, Risk Management Officer, and F2OnSite Department Heads.

IV. Policy

Per the Risk Management Policy, executive management shall be involved in risk management and mitigation decisions including how security processes are communicated throughout the organization.

Security self assessments help manage and reduce risks to F2OnSite's Information Resources. The Chief Security Officer (MGMT), with assistance from the Risk Management Officer (RMO), shall oversee the security self assessment. Security self assessments shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The MGMT shall:

- Resources – identify internal resources to perform the security self assessment.
- Scope – define the scope of the security self assessment.

- Security Requirements – prepare a list of any requirements that are relevant to the security self assessment.
- Description – Describe the Information Resources to be assessed including mission description, system identification, and criticality. Describe the environment including facilities, physical security, maintenance, etc. Identify the system architecture, interfaces, data flow, etc. Describe the system security requirements.

The MGMT shall identify the security safeguards to be included in the security self assessment project scope:

- Administrative safeguards – identify if administrative safeguards are to be included in the scope. Administrative safeguards include security policies, procedures, job descriptions, agreements with service providers, security training and awareness plans, incident response plans, business continuity plans, cyber security insurance policies, and other written security controls.
- Technical safeguards – identify the technical safeguards to be included in the project scope. Technical safeguards include access controls (passwords, account lock, inactivity timeout), security protection measures (firewalls, anti-malware, encryption), management (patch management, system utilization, backups), logging and monitoring systems, system configurations and hardening, and related security controls.
- Physical safeguards – identify the physical safeguards to be included in the project scope. Physical safeguards include secure areas are protected by appropriate entry controls, only authorized personnel are allowed access, cameras record activities in sensitive areas with appropriate retention of images, procedures identify visitor controls such as visitor sign-in, wearing of visitor badges, escorting by authorized personnel, etc.

Once the scope has been identified, the MGMT shall:

- Vulnerabilities – establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”).
- Evaluating – identify methods for evaluating vulnerabilities and assigning risk ratings based on an organization’s environment and risk assessment strategy.
- Tools – ensure access to security assessment tools is controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. Security self assessment requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

The security self assessment report shall include the project scope, findings, and recommendations to enhance security. The MGMT shall:

- Review the report to confirm the findings and verify the security recommendations are appropriate and sufficient.
- Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The Risk Management Officer shall provide necessary reporting to F2OnSite Executive Management.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to F2OnSite Executive Management, Chief Security Officer, Risk Management Officer, and F2OnSite Department Heads.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	

References:

COBIT EDM03.07, APO11.09, APO13.07, BAI04.05, BAI10.07, DSS05.08, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(8)
ISO 27001:2013 8.3, 9.2, 9.3, A.12.7, A.15.2.1
NIST SP 800-37 3.5, 3.7
NIST SP 800-53 3.3, AU-1, AU-6
NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-1-4
PCI Self-assessment Questionnaires (SAQs), A3.1.2

SERVER CERTIFICATES POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

The need to communicate securely over public lines and the Internet resulted in the development of the Public Key Infrastructure (PKI) framework. PKI utilizes public-key cryptography and digital certificates to enable information to be sent in a secure and confidential manner.

II. Purpose

Certificate Authorities (CA) sign and distribute certificates used to assure an identity when establishing encrypted communications. The purpose of this policy is to ensure proper controls are in place related to the selection of providers of trusted server-side third-party certificates and their implementation within F2OnSite Information Resources.

III. Scope

This policy applies to IT Department Staff responsible for administering and securing Information Resources.

IV. Policy

Certificates are most commonly used for secure (https) Web sites. Web browsers inspect signed server-side certificates to verify that a Web server is authentic, using a specific Uniform Resource Locator (URL), and that the URL has been publicly verified with the identity of the institution. Using a server certificate helps assure the integrity and confidentiality of the encrypted communications through the use of cryptographic protocols such as Transport Layer Security (TLS).

Other types or classes of certificates may be installed on the client side web browser and used for the legal non-repudiation of transactions and multi-factor authentication, such as when the specific identity of individuals needs to be validated when connecting the server.

F2OnSite's IT Department shall ensure security controls protect sensitive communications by encrypting communication channels between endpoints using Transport Layer Security (TLS), or equivalent cryptographic protocols. Secure Hypertext Transport Protocol (HTTPS) connection based on server-side certificates shall be signed by a trusted third-party certificate provider.

To ensure that the security and integrity of the certificate remains intact, solutions must be installed and maintained according to the provider's instructions and recommended use. Any deviation from the provider's instructions or recommended use must be approved by the Director of IT and the Chief Security Officer.

Where possible, newer versions of TLS shall be used to protect authentication and communications against eavesdropping and tampering.

The use of wildcard certificates for one or more subdomains within the F2OnSite domain is permissible under the following conditions:

- The service provided by the system may not be used to store or access sensitive data
- All requests for wildcard certificates are approved by the Director of IT prior to certificate purchase, acquisition or assignment.

Network administrators shall track certificate expiration dates to ensure that certificates are kept current and an expired certificate does not adversely impact business operations.

Self-signed certificates are only permitted for development systems that are segregated from the F2OnSite production network and are not connected to external resources (e.g. Internet).

Network administrators shall comply with F2OnSite's Server Hardening Policy to ensure systems are protected from security and performance issues.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Department Staff responsible for administering and securing Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	7/1/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO12.02, APO13.07, BAI02.05, BAI04.05, BAI05.09, BAI06.06, DSS04.07, MEA01.05

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv), 164.312(e)(2)(ii)

ISO 27001:2013 6.1.3, A.10, A.18.1.5

NIST SP 800-37 3.3, 3.4, 3.7

NIST SP 800-53 IA-7, SC-12, SC-13, SC-17

NIST Cybersecurity Framework ID.RA-6, PR.AC-3, DE.DP-2

PCI 2.1.1, 2.3, 3.4.1, 3.5-6, 4.1, 4.3, 6.5.3-4, 8.2.1

SERVER HARDENING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite must protect servers from both security and performance issues. Servers are depended upon security to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

II. Purpose

The purpose of this policy is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

III. Scope

This policy applies to all individuals responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource security.

IV. Policy

A server must not be connected to the F2OnSite network until it is in an F2OnSite accredited secure state and the network connection is approved by F2OnSite IT security Staff.

A Server Hardening Procedure shall provide the detailed information required to harden a server and must be implemented for F2OnSite IT accreditation. At a minimum, the Server Hardening Procedure shall include:

- Installing the operating system from an IT approved source
- Applying vendor supplied patches

- Removing unnecessary software, system services, and drivers
- Setting security parameters, file protections and enabling audit logging
- Disabling or changing the password of default accounts

F2OnSite IT security Staff will monitor security issues, both internal to F2OnSite and externally, and will manage the release of security patches on behalf of F2OnSite.

Where practical, F2OnSite's IT Department will test security patches against IT core resources before installing in production environments.

In the case of special applications, F2OnSite's IT Department may make hardware resources available for testing security patches.

Critical security patches must be implemented within the specified timeframe (typically 30 days) of notification from F2OnSite's IT Department.

To minimize risks, each server shall have only one primary function (e.g. E-mail, database, Human Resources).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Department Staff and the Chief Security Officer.

Policy History

Version	Date	Description	Approved By
2.1	07/1/2020	Updated Initial policy release	D Lauderback

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)
ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14
NIST SP 800-37 3.3, 3.4
NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10
NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1
PCI 2.1-3, 2.5-6, 4.1, 5.1, PCI Software Security Framework

SERVER HARDENING PROCEDURE

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Server policies provide management direction and guidance to ensure systems and data are properly protected. Procedures document a detailed description of the steps necessary to perform specific operations that comply with F2OnSite's server related policies.

II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in F2OnSite's Server Hardening Policy.

III. Scope

This procedure applies to IT Department Staff who administer servers.

IV. Procedure

Physical security. Ensure the server is placed in a physical location that restricts access to authorized individuals. Where possible, consider a locking cabinet/rack in a secure data center.

Alerts, advisories, and vulnerability announcements. Monitor manufacturer alerts, advisories, and vulnerability announcements. Ensure patches and updates are installed at the time a new server is placed into production and on-going per the Patch Management Policy.

Logging and monitoring. Ensure logging is activated per the Logging Policy. Consider centralized logging that consolidates logs for analysis and incident tracking. Log messages may be assigned a severity level whereby specific messages, based on their severity, are sent to remote logging servers. By default, these messages may be transmitted in clear text. Where possible, encryption should be used when transmitting messages.

Domain. If the server is part of Active Directory, most policies will be configured at the domain level. Stand-alone servers can be configured in the local policy editor.

Accounts. Where possible, disable the local Administrator account. For accountability purposes, ensure each Network Administrator uses a unique account/logon. Ensure local guest accounts are disabled.

Passwords. Ensure default credentials are changed. Ensure a long and complex memorized secret (i.e. password) is used to administer the device and complies with the Password Policy. When changing a password, ensure users cannot enter a recent prior password (password history). See the Password Policy for more information.

Account lock. Ensure accounts are locked out after five consecutive failed (invalid) logon attempts within a 24 hour period. The lockout duration shall be at least 30 minutes or until a system administrator re-enables the user ID. Refer to the Securing Information Systems Policy for more information.

Inactivity. Ensure users are automatically logged off after 15 minutes of inactivity. Refer to the Securing Information Systems Policy for more information.

Network configuration. Where possible, configure two Domain Name Servers (DNS) in the event one of the servers fails or is unable to provide services. Production servers should have static IP addresses. Remove unneeded packages/applications and disable unneeded services and drivers.

Firewall. As a general rule, each server should have a software firewall activated on the device. The software firewall helps protect against network based attacks.

Time. An accurate time and date is important for system and event logs. Configure a trusted time source for Network Time Protocol (NTP) and use proper authentication.

Anti-Malware. Ensure the device is protected from malicious software such as viruses, worms, Trojan Horse programs, etc. Ensure the Malware software and definitions are updated in a timely manner. Refer to the Anti-Malware Policy for more information.

Testing. Where possible, the server should be tested prior to installing the device in a production environment.

Management sessions. Administrators should not connect to the device using unsecure services where communications are not encrypted. Ensure only authorized personnel are allowed to access and administer the device.

Warning banners/notices. Some implementations may require the use of warning banners or notices. Network administrators should consult with F2OnSite legal staff regarding the posting of notices such as:

- Access is only permitted by authorized personnel
- Activities are logged and monitored and can be used as evidence
- Unauthorized access or use can result in civil and criminal penalties

Backup. A copy of the device configuration should be saved at a separate and secure location to assist in a recovery effort if needed.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening servers and specific security functionality.

V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Department Staff who administer servers and the Chief Security Officer.

Procedure History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial procedure release	

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)
ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14
NIST SP 800-37 3.3, 3.4
NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10
NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1
PCI 2.1-3, 2.5-6, 4.1, 5.1

SMARTPHONE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Today's Smartphones include advanced features such as the ability to connect to the Internet, download applications, take videos, use wireless connectivity, access network data, etc. While Smartphones increase productivity, they also come with risks.

II. Purpose

The purpose of this policy is to help manage Smartphone related risks Staff members and F2OnSite.

III. Scope

This policy applies to all F2OnSite Staff that use Information Resources.

IV. Policy

Only IT Department approved Smartphones may be used to access F2OnSite networks and Information Resources.

F2OnSite uses a multi-layered approach to protecting Smartphones and related "information assets". Securing Smartphones is the responsibility of both the phone user as well as F2OnSite's IT Department.

User activities can download malware to a Smartphone. Once installed, the malware can launch attacks against F2OnSite's internal network. Staff security education and awareness training should be provided on a regular basis. Staff should only download and install applications from trusted sources. In addition, Staff should not click on message links from unknown senders or visit unknown web sites.

To reduce IT administration costs and offer better protection for the enterprise, F2OnSite's IT Department shall establish standards for Smartphones and security

protection software. Smartphone protection software should be installed on all devices that access the Internet and especially Smartphones that access F2OnSite's Information Systems. If possible, the IT Department shall use a single console to protect and manage Smartphone devices. Smartphone security protection software shall include the following features:

- Protection against Malware
- Periodic scan of installed applications to ensure they are safe
- Block malicious websites that can compromise the device
- Identify applications that allow access to user private information
- Remotely wipe Smartphone data in the event the device is lost or stolen
- Block web-based Malware and phishing attacks by scanning e-mails and text messages

Smartphones shall have a very strong password and a short screen timeout. This helps prevent an unauthorized person from downloading and installing unwanted applications.

The F2OnSite IT Department shall perform periodic risk assessments to identify, manage, and reduce Smartphone related risks and access to Information Resources. Refer to the Risk Assessment Policy for more information.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from Smartphones which are generally higher-risk than non-portable devices (e.g., desktop computers).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO10.05, APO12.02, APO13.07, BAI02.05, BAI03.05, DSS01.05, DSS05.02

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001:2013 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-1, ID.GV-4, ID.RA-4, PR.AC-1-4, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2

SOCIAL NETWORKING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Social network services are used by individuals and organizations to meet, establish, and maintain relationships with others. In business, F2OnSite's sales department uses social network services to convey information about new products and services and to solicit customer feedback. This policy recognizes that social network services are integral to F2OnSite operations.

II. Purpose

Social network services can create risks to the individual and F2OnSite. The purpose of this policy is to address the responsible and effective use of social network and social media services.

III. Scope

This policy applies to all F2OnSite Staff that have access to F2OnSite Information Resources.

IV. Policy

Publically accessible information systems are not owned, operated, or controlled by F2OnSite. This Policy applies to collaborative tools such as social network services, social media, user generated content, and social software including, but not limited to, Facebook, Twitter, MySpace, YouTube, MetaCafe, Google Apps, Wikis, blogs, and similar collaborative and information sharing Social network services where users can add or generate content.

The appropriate department head must give consent on the planned use of social networking services. Where appropriate, a risk assessment should be performed to determine the Internet based service assets, threats, vulnerabilities, and impact on F2OnSite. The department head will:

- Approve the establishment of official external presences on Social network services.
- Ensure the role and scope of the Internet based service is clearly documented.
- Ensure the Internet based service is monitored and periodically evaluated for compliance with security requirements, fraud, and/or objectionable material.
- Ensure that the information posted is relevant and accurate and only provides information approved for public release.
- Ensure the Internet based service includes a disclaimer when personal opinions are expressed.
- Ensure users of Social network services are aware of the potential value of the content.

As a general rule, department heads will not approve the following types of information to be posted on social network services:

- Conversations between Staff members.
- Announcements, documents, discussions, or other information shared in internal meetings.
- The names of clients, partners, suppliers, or other Staff.
- Internal e-mails, notes, memos, and other interpersonal communications.
- Internal documents not specifically marked for external distribution.
- Pre-publication drafts of documents ultimately intended for public distribution.
- Planning documents or production documents.
- Software code.
- Organizational charts (org charts)
- Organizational contracts, policies, and other legal documents.

In general, department heads may allow the following types of information to be freely disclosed:

- Information published on unprotected sections of F2OnSite's web site.
- Information published by F2OnSite's Public Relations department.
- Publicly available business information.
- Advice and general professional insight that does not expose internal operational procedures or imply or disclose any proprietary or otherwise protected information.

The IT Department is responsible for providing and managing Internet connectivity. IT shall be responsible for protecting F2OnSite Staff, equipment, and data from malicious software and activity. IT will take immediate actions are required to preserve information confidentiality, availability, and integrity. IT will deny access to sites with prohibited content and prohibit users from engaging in unapproved activity via social

networking sites. Prohibited activity includes pornography, gambling, hate crimes, and related activity.

When accessing Social network services, in an authorized personal or unofficial capacity, F2OnSite Staff shall employ sound operations security measures as indicated below:

- Settings: to protect privacy, apply the appropriate restrictions and settings provided by the social network sites. Monitor social network privacy changes and features. Change privacy settings to “friends only” so that hackers cannot see profile information.
- Security awareness: educate F2OnSite Staff on the dangers of clicking on links in text messages and e-mail. Know how to detect false profiles and fake e-mail messages.
- Friends: take care when accepting friend requests in case the profiles in question are fakes. Most hackers don't have time to create long and interesting profiles. Also, it is probably a fake if they have lots of friends and have only had a profile a short amount of time.
- Disclosure: revealing too much information about yourself or your organization creates risks. Remove any sensitive information you do not want disclosed to others. Organizations should implement social networking policies dictating who in your organization is permitted to post information, the type of information that can be posted, how it is to be managed, and how the organization's on-line social identity and intellectual property will be protected.
- Smartphones and Wearable Computing Devices: in some cases the device has been programmed with the password to social networking sites. This makes it easy for the user but also makes it easy for a hacker. Ensure your device has a password lock or other security mechanism.
- Protection software: ensure all devices used to access social networking sites have malware protection. This includes anti-virus and anti-spyware protection. Some protection software includes the ability to remotely wipe a Smartphone or Wearable Computing Device if it is lost or stolen.
- Patch management: ensure your application, operating system, third party software (pdf readers, flash, etc.), and web browsers are patched and updated on a regular basis.
- Incident response: notify social network security teams if you detect suspicious activity. The security teams can remove infected pages and apply filters to restrict future activity.
- Privacy policy: read and understand the privacy policy posted on the social network. If you don't agree to their terms, don't use their service.

Official uses of social network services are permitted, however, because these interactions take place in a public venue, F2OnSite Staff shall maintain a liaison with the Legal Department and IT security to ensure organizational awareness and controls. IT Security shall:

- Maintain a registry of official external presences on Social network services.
- Develop and maintain threat estimates on current and emerging Social network services.
- Integrate guidance regarding the proper use of social network services into Staff training and awareness activities.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	1/1/2020	Initial policy release	D LAUDERBACK

References:

COBIT EDM01.04, APO07.01, APO11.07, APO12.02, DSS01.04, DSS06.04, MEA03.04
GDPR Article 25, 32
HIPAA 164.308(a)(1)(i), 164.308(a)(2)
ISO 27001:2013 6.1.3, 8.3, 9.1, A.5.1.1, A.6.1.2, A.7.2.1, A.8.1.3
NIST SP 800-37 3.2, 3.4, 3.7
NIST SP 800-53 AC-5, PL-4, PS-6, PS-7, SA-9
NIST Cybersecurity Framework ID.AM-6, ID.GV-3, ID.RA-6, PR.AC-4, DE.CM-3, DE.DP-2
PCI 3.7, 6.1, 7.1, 8.1, 8.4

SOFTWARE DEVELOPMENT POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Implementing solid security policies, blocking unnecessary access to source code, implementing testing procedures, and managing the transfer of software from development to production helps mitigate F2OnSite's software development risks.

II. Purpose

This policy describes the requirements for developing, implementing, acquiring, and managing the software development life cycle.

III. Scope

This policy applies to all Staff that manage and provide software development services.

IV. Policy

A. Software Development Life Cycle (SDLC)

The IT Director is responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, SDLC should address the following ten areas:

11. Feasibility study
12. Risk assessment
13. User requirements
14. Systems design
15. Programming or acquire software (development/acquisition)
16. Quality assurance
17. Documentation
18. Systems testing and acceptance
19. Installation

20. Maintenance through disposal

The SDLC methodology ensures that the software will be adequately documented and tested before it is used for critical business processes and storing of information.

B. Access Controls

All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) must be assigned for all production systems.

Software protection mechanisms shall be developed to protect the confidentiality, integrity, and availability of critical assets and sensitive data.

There shall be a separation between development, testing, and operational environments to reduce the risks of unauthorized access or changes to the operational environment. This ensures that security is rigorously maintained for the production system, while the development, and test environments maximize software development productivity.

- Software development staff must not be permitted to have access to production systems and related data.
- Development systems must not contain sensitive or confidential information.

Access to program source code shall be restricted to authorized personnel.

Prior to moving software into production:

- All application-program-based access paths other than the formal user access paths must be deleted or disabled.
- Software debugging code must be removed.
- Test user IDs and passwords must be removed.
- Custom code shall be reviewed prior to release to identify any potential coding vulnerability. Secure coding practices shall be appropriate to the programming language and development environment. Code changes shall be reviewed by individuals other than the originating code author and by individuals knowledgeable about code-review techniques and secure coding practices. Such review to ensure code is developed according to secure coding guidelines and appropriate corrections are implemented prior to release. Code review results are reviewed and approved by IT management prior to release. The requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews shall be conducted by knowledgeable internal personnel or third parties. Public-facing web applications

are also subject to additional controls, to address on-going threats and vulnerabilities after implementation.

The IT Department's operations Staff will move programs from development into production. Software developers shall not be permitted to move programs into the production environment.

F2OnSite's IT Department must perform periodic risk assessments of production systems to determine whether the controls employed are adequate. Procedures shall be developed controlling the risks related to systems development access during emergencies (program aborts, etc.). Refer to the Risk Assessment Policy for more information.

C. Data Owners

All production systems must have designated Owners and Custodians for the critical information they process.

Data owners shall review test results and provide approval prior to moving new software or software updates into production. Data owners shall also review and approve data migrations from one application or system to another.

D. Quality assurance

The development of all software shall be supervised and monitored by the organization and must include security requirements, independent security review of the environment by a Certified Information Systems Auditor, certified security training for software developers, and code reviews.

Applications shall be securely designed, coded, and maintained per the Secure Software Development Lifecycle Policy. Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and comply with applicable regulatory and business requirements.

Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data.

Quality assurance procedures shall include systematic monitoring and evaluation of software developed, outsourced, or acquired by F2OnSite. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented and tests of the system(s) shall be carried out both during development and prior to acceptance to maintain security. Refer to the Quality Assurance Policy for more information.

Test data shall be carefully selected, protected, and controlled. Management shall have a clear oversight capacity in the quality testing process with the final product being certified as:

- Fit for purpose - the product should be suitable for the intended purpose, and
- Right first time - mistakes should be eliminated prior to release.

Static and dynamic analysis tools shall be used to verify that secure coding practices are being adhered to for internally developed software:

- Static testing - application data and control paths shall be modeled and then analyzed for security weaknesses. Static analysis shall test the internal structure of the application, rather than functional testing.
- Dynamic analysis of a program/application shall occur when it is in operation.

Procedures shall control the risks related to production software and hardware changes that may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications. This includes:

- Separate development/test environments from production environments and enforced accesses controls.
- Separation of duties between development/test and production environments.
- Production data (e.g. live Primary Account Numbers, Names, etc.) is not used for testing or development.
- Where appropriate, processes exist for the removal of test data and accounts before production systems become active.
- Change control procedures for the implementation of security patches and software modifications include: Documentation of impact, change approval by authorized parties, functionality testing to verify that the change does not adversely impact the security of the system, and back-out procedures.

E. Software Security

The Chief Security Officer (MGMT) shall ensure secure software requirements:

- Staff implement secure software lifecycle management practices.
- Processes exist to identify, assess, and manage threats and vulnerabilities to the software.
- Secure software releases and updates are provided in a timely manner.
- Appropriate personnel provide clear and thorough guidance on the secure implementation, configuration, and operation of the software.

The MGMT shall ensure secure software lifecycle requirements:

- A formal software security governance program establishes responsibility and authority for the security of software products and services. Resources are allocated to execute the strategy and ensure that personnel are appropriately skilled. Staff define, maintain, and communicate a software security policy and a strategy for ensuring the secure design, development, and management of

software products and services. Performance against the software security strategy shall be monitored and tracked.

- Staff shall continuously identify, assess, and manage risk to the software and services. Staff shall detect and mitigate vulnerabilities in the software and its components to ensure that software remains resistant to attacks throughout its entire lifetime.
- Staff shall identify and manage software changes throughout the software lifecycle. Staff shall protect the integrity of the software throughout the software lifecycle. The confidentiality, integrity, and availability of Sensitive Information shall be maintained.
- Staff shall provide clear and thorough guidance on the secure implementation, configuration, and operation of software applications. Staff shall maintain communication channels with Data Owners regarding potential security issues and mitigation options. Staff shall provide Data Owners with detailed explanations of all software changes.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to the Chief Security Officer and all Staff that develop, implement, acquire, or manage software development.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO01.03, APO01.11, APO05.05, APO12.07, APO13.07, BAI03.05, MEA02.11
 GDPR Article 25, 32
 HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(2)
 ISO 27001:2013 5.2, 6.2, A.14
 NIST SP 800-37 3.2, 3.4
 NIST SP 800-53 PL-2, PL-7, PL-8, SA-3, SA-4, SA-15, SA-17
 NIST Cybersecurity Framework ID.AM-6, ID.GV-3-4, ID.RA-6, PR.IP-2-3, PR.MA-1
 PCI 6.1-7, PCI Software Security Framework

SOFTWARE LICENSING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws.

II. Purpose

This policy establishes the rules for licensed software use on F2OnSite's Information Systems.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

F2OnSite provides a sufficient number of licensed copies of software so that Staff can perform the duties in an expedient and effective manner. Management must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed for business activities.

Third party copyrighted information or software, that F2OnSite does not have specific approval to store and/or use, must not be stored on F2OnSite Information Systems. Systems Administrators will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).

Third party software in the possession of F2OnSite must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

If permitted in the license agreement, Staff may copy an image of the software onto a computer file server for the purpose of downloading and installing the software onto computers within the same network.

If the license agreement permits a copy for a secondary or home computer, Staff may copy an image of the software for such purpose providing that Staff remove such copy on the secondary or home computer when employment with F2OnSite is terminated.

If the software license agreement permits copying without restrictions on a number of devices, Staff may copy an image of the software for such purpose as long as Staff remains within the number of permitted devices/copies.

Software may be designated as trial or evaluation versions. Staff may install and use this type of software only during the trial or evaluation period and only for specified purposes.

All installations of software on company equipment must be performed by IT Department Staff. Per the Acceptable Use Policy:

- Only the IT Department is authorized to install software on servers, storage, and other related Information Resources.
- Installation of software without approval from F2OnSite management is unauthorized.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff that use F2OnSite Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	7/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO01.03, APO05.05, APO10.05, APO12.02, APO12.07, BAI04.05, DSS04.05
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(3)(ii), 164.308(a)(4)(ii)(C)
ISO 27001:2013 6.1.3, 8.3, 9.1, A.8.1.1, A.8.1.3, A.8.3.1, A.9.1.2, A.9.4.1
NIST SP 800-37 3.3, 3.7
NIST SP 800-53 AC-2-3, AC-6, CM-8, MP-2, MP-4, MP-5, MP-6, MP-7, PL-4
NIST Cybersecurity Framework PR.AC-1, PR.AC-3-4, PR.AT-1, PR.PT-2, DE.DP-2
PCI 2.2, 2.4, 7.1-2

STAFFING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite must have appropriately supervised professional Staff sufficient to maintain business processes. The staffing level should be appropriate to the environment considering the amount and type of information for which they are responsible as well as the level of risk.

II. Purpose

This policy ensures sufficient Staffing resources are allocated to supporting and managing F2OnSite business processes.

III. Scope

This policy applies to all F2OnSite Department Heads.

IV. Policy

F2OnSite departments are responsible for having appropriately supervised professional staffing sufficient to maintain business processes. The staffing level should be appropriate to the environment considering the amount and type of information for which they are responsible as well as the level of risk.

Staffing processes generally involve the following four steps which apply equally to general users as well as to managers, System Administrators, and security personnel.

1. Position definition - early in the process of defining a position, security issues must be identified and addressed. Once a position has been broadly defined, the responsible Department Head must determine the type of computer access needed for the position. Security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for a particular information system shall be determined by the clearance level, formal access approvals,

and need-to-know held by users of the information system, and the classification level of data processed or stored. There are two general security rules to apply when granting access:

- Separation of duties. Refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.
- Least privilege access. This means of granting access refers to the security objective of granting users only those accesses they need to perform their official duties. Data entry clerks, for example, may not have a need to run E-mail utilization reports.
- Competency. Management shall determine the necessary competency of Staff that affects information security performance and determine the competency needed based on the appropriate education, training, or experience.

2. Position sensitivity – the responsible Department Head shall determine the position sensitivity, based on the duties and access levels, so that appropriate cost effective screening can be completed.

3. Screening – management shall take actions to acquire and maintain Staff with the necessary competence. Background screening helps determine whether a particular individual is suitable for a given position. Generally, it is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening alone to reduce the risk to F2OnSite. Pursuant to local laws, regulations, ethics, and contractual constraints all employment candidates, contractors and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Contractual agreements shall state Staff and F2OnSite's responsibilities for information security.

4. Training and awareness – Staff shall be trained in the computer security responsibilities and duties associated with their jobs. Refer to the Security Training Policy for more information.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to Executive Management and Department Heads.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO07.12-13, APO08.12-13, APO10.05, APO11.09-10, APO12.07, BAI08.11-12

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i)

ISO 27001:2013 8.1, A.6.2.2, A.7.1, A.9

NIST SP 800-37 3.4, 3.6, 3.7

NIST SP 800-53 AC-1-3, AC-17, PE-17, PL-4, PS-6, PS-7, SA-9

NIST Cybersecurity Framework ID.AM-6, ID.RA-6, PR.AC-1-4, PR.AC-6-7, PR.AT-1, DE.DP-2

PCI 7.1-3, 8.1-2, 8.4-5, 8.8

SYSTEM AND ORGANIZATION CONTROLS (SOC 2) POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.0

I. Overview

Security controls and safeguards are part of F2OnSite's risk management process to mitigate, eliminate, and transfer risks that can impact business operations.

II. Purpose

Service and Organization Controls (SOC 2) audits evaluate service provider risks and help ensure F2OnSite's controls are sufficient and effective.

III. Scope

This policy applies to all F2OnSite Department Heads, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

IV. Policy

An independent audit assists the Chief Security Officer (MGMT) and Risk Management Officer (RMO) in ensuring that controls and safeguards are appropriate, sufficient, and effective at treating risks. The auditor evaluates systems for best practices and compliance with an established set of requirements.

The MGMT shall define the scope of the audit. SOC 2 audits focus on evaluating controls grouped into one or more of the following Trust Services Criteria:

- Security – a common criteria that applies to all audits and must be included except for a Privacy Audit. The Security criteria includes protection against unauthorized logical or physical access, use, or modification.
- Confidentiality – evaluates protection of Sensitive Information including unauthorized access, protection of data, agreements with clients, etc.

- Availability – systems are available when needed and according to agreed upon criteria and requirements such as those stated in contracts and Service Level Agreements (SLA).
- Processing Integrity – validates transactions and related processing are complete, error free, timely, and accurate. Data cannot be modified in an unauthorized or undetected manner.
- Privacy – a Privacy Audit evaluates how F2OnSite collects and uses personal information. This audit evaluates data handling contractual obligations, F2OnSite's Privacy Policy, and related laws and regulations.

Based upon the scope of the audit, the MGMT will identify resources to perform the SOC 2 audit.

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

SOC 2 audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources.

The auditor's report shall include their project scope, findings, and recommendations to enhance compliance. The MGMT shall:

- Review the security auditor's report to confirm the findings and verify the recommendations are sufficient and effective.
- Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The MGMT shall document important findings in the Audit Log Form and the RMO shall provide necessary reporting to F2OnSite Executive Management.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
1.0	03/01/2020	Initial policy release	D Lauderback
2.0	07/01/2020	Updated Policy Release	D Lauderback

References:

COBIT EDM03.02, APO01.03, APO01.11, APO12.02, APO12.07, MEA03.01, MEA04.11
GDPR Article 32
HIPAA 164.308(a)(8)
ISO 27001 9.2, A.15.2.1
NIST SP 800-37 3.5
NIST SP 800-53 3.3, AC-5, AU-6, CA-2
NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2
PCI 2.2.a-d

SYSTEM SECURITY PLAN

I. Purpose of the System Security Plan

The purpose of the System Security Plan (Plan) is to provide an overview of the security requirements of F2OnSite's Information Resources. This Plan also describes the controls necessary to ensure information availability, confidentiality, and integrity.

II. Overview of the System Security Plan

The System Security Plan documents our structured process of planning adequate and cost-effective security protection. It reflects input from managers and asset owners, the IT Department, and F2OnSite's Chief Security Officer (MGMT).

F2OnSite's System Security Plan leverages our existing security policies, procedures, and plans including:

- Risk Assessment
- Risk Assessment Policy
- Risk Management Policy
- Risk Task List
- Risk Treatment Plan
- Security Controls Review Policy
- Security Policy

III. Security Policy

F2OnSite's Security Policy provides overall guidance and direction for information security and related activities.

Security plans are no longer a luxury, but an essential element of F2OnSite's risk management program. The decision to invest in security is required by legislation, third parties (e.g., insurers), and the realistic view that management must minimize the impact of security incidents on business operations.

F2OnSite's Security Policy is in place to protect F2OnSite and its information assets. Risk Assessments and Risk Treatment Plans ensure that risks are identified and the appropriate mitigating technologies are in place.

An up-to-date Security Plan creates a competitive advantage out of its ability to respond to rapid changes in the environment. F2OnSite can then move from simple firewalls and anti-virus solutions to experiencing the benefits associated with the continuing of business operations that are in line with the corporate strategy of facilitating growth and profitability.

IV. Risk Assessment

F2OnSite is committed to protecting its business operations, investments by its stakeholders, and assets of the organization. Risks assessments are used as a tool to help identify and mitigate risks to assets.

F2OnSite management defines and selects the risk assessment methodology and approach considering internal and external risk assessment resources. A significant amount of risk assessment, planning, and knowledge of security controls is required. This ensures that the proper level of security is designed and implemented properly.

The purpose of the risk assessment is to determine areas of vulnerability and minimize risks to the organization. These risk assessments are concentrated on business processes and related assets that are of a high priority and importance to the organization.

While preparing and conducting a risk assessment, the following best practices or approaches should be considered.

A. Assets

One of the first steps is to identify important assets. This includes facilities, network infrastructure components, customer data, intellectual property, etc. Without a complete and accurate inventory of IT assets, criticality and impact on the organization cannot be determined.

Depending on the accuracy and availability of inventory documentation and asset valuation data, F2OnSite may need to conduct an asset valuation or asset criticality (importance) assessment to prioritize and determine those network infrastructure components and assets that are most important to the organization.

B. Threats

Once the assets are inventories, the risk assessment identifies general and specific threats to the assets. Threats can include both unintentional and intentional threats including:

- Natural threats (acts of God)
- Accidental or unintentional threats (staff error, equipment failure, etc.)

- Intentional threats such as asset theft and asset tampering (malicious damage)

C. Vulnerabilities

Threats identify realistic events with a potential harm to the organization. The risk assessment identifies vulnerabilities or weaknesses that allow a threat to be exploited. For example, an imposter posing as an employee is a threat and related vulnerabilities can include physical access to systems, lack of employee security related education, etc.

D. Impact

Once assets, threats, and vulnerabilities are identified, the risk assessment will evaluate the potential impact or loss on our organization. Examples included the impact on our ability to perform services and meet deadlines. It also includes a negative impact on revenue, damage to our image and reputation, etc.

V. Risk Analysis

Once the risk assessment identifies our assets, threats, and vulnerabilities, a risk analysis determines the potential impact on our organization. Each asset includes the following information:

- Asset class – major asset grouping (e.g. Information Technology).
- Asset – specific asset (e.g. Servers).
- Threat – potential to cause harm to an asset (e.g. unsecured data center)
- Vulnerability – a weakness that could be used to exploit a threat (e.g. theft)
- Impact – loss (e.g. customer data exposed results in lost revenues)

Risk reduction is the process of identifying measures and controls to safeguard against the above risks and impact on our organization. Risk reduction evaluates potential risks and safeguards:

- Physical risks - we determine the vulnerability of the data center and the impact of environmental hazards on the computer, related equipment, and contents.
- Communication risks - we evaluate the system for threats to the privacy and authenticity of telecommunications.
- Hardware - we review the system's current or proposed hardware configurations.
- Software - we review operating and application software for security risks and potential vulnerabilities.
- Personnel - we describe staffing and third party risks and potential vulnerabilities.

We then identify various risk treatment safeguards and controls for appropriateness, cost

efficiency, and effectiveness. Risk reduction strategies include safeguards and controls to:

- Mitigate – implement controls to reduce risks to an acceptable level
- Transfer – transfer risks to another entity
- Eliminate – change the business model to avoid or eliminate the risk if the risk cannot be reduced to an acceptable level or transferred to another entity
- Monitor – acknowledge the risk and monitor to ensure the risk remains within acceptable limits

VI. Risk Response

In most instances, F2OnSite reduces risks through the use of mitigating controls and safeguards. For each applicable risk, we implement safeguards to enhance the effectiveness of our controls to prevent and minimize the threat or vulnerability. In some instances, insurance transfers the risk to an outside entity.

It should be noted that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A separate Risk Treatment Plan describes how we manage risks. It defines roles and responsibilities for participants in the risk processes, the risk reduction activities, the schedule for risk management activities, and any techniques used.

The Risk Treatment Plan is updated on an on-going basis as tasks are completed and new risks are identified. The Risk Treatment Plan identifies how the Risk Task List is maintained and risk resolution status is reported to management.

Appendix A – Distribution List

President

Chief Operating Officer

IT Director

IT security Staff

Chief Security Officer

Appendix B – Receipt and Acknowledgement

I have read F2OnSite's (Company's) System Security Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)

SYSTEM UPDATE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

This policy is an internal IT policy which defines how often and under what conditions computer system updates are performed.

II. Purpose

This policy establishes a minimum process for protecting Staff from security vulnerabilities. This policy, when combined with the Patch Management Policy, determines how updates are to be performed for both servers and workstations.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

This policy defines methods used to determine what updates should be applied as well as the timing of the updates.

A. Update Monitoring

Several types of computer updates should be monitored:

- The computer BIOS.
- The operating system.
- Software application updates.
- Miscellaneous updates (e.g. Flash, Adobe Reader).

There are several methods that can be used to determine when updates should be performed:

- Review of posted security flaws and patches for each type of update applicable to the computer system.

- An automatic scanning of the system to determine available updates not yet applied to the system or application.
- The review of posted security flaws and patches should always be used for the computer operating system, BIOS, and applications. The manufacturer website should be used and there may also be other appropriate sites posting relevant bulletins. If automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

Procedures shall be developed to:

- Determine how to identify appropriate patch or configuration changes for F2OnSite's servers and workstations. Updates for servers shall be checked no less than monthly to determine whether any new updates are required.
- Ensure that appropriate patch or configuration change works as desired without causing other disruptions. Where possible, a test environment should be used to determine whether updates may break production functionality.
- Prioritize updates and patches if several patches need to be applied.

B. Update Preparation

Before approving updates, System Administrators should understand:

- The addressed vulnerability.
- Previous patches or system update required.
- Programs affected by the change.
- Problems that may result as a result of the change.
- Procedures to back out or undo the change.

All patches approved for client computers shall be documented prior to release. When possible, new patches shall be tested in a controlled environment that mimics the infrastructure of the production environment before patches are applied.

IT Staff shall ensure that backups exist of applications and data prior to installing a patch or update. Each server shall have documentation that identifies the list of applications running on the device as well as a patch history.

C. Applying Updates

Depending upon the type of device, operating system, and criticality, workstation updates may be performed manually, using tools, or automatic updates. Automatic updates can save a great deal of time and expense since all workstations can be updated at the same time. All workstations shall have current versions of the operating systems.

Server updates shall be performed by a qualified and authorized System administrator after the update has been tested in a non-production environment. Assuming software compatibility, servers shall have current versions of the operating systems.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for maintain servers and workstations.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	

References:

COBIT APO05.03, APO05.05, APO11.09-10, BAI06.02, BAI06.05-06, BAI07.06, BAI10.07
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.310(c)
ISO 27001:2013 A.11.2.4, A.11.2.6, A.12.1.2, A.12.6
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 RA-3, RA-5, SI-2, SI-5
NIST Cybersecurity Framework ID.RA-2, ID.RA-6, ID.RM-1, PR.IP-3, DE.DP-2
PCI 6.1, 6.2

TERMS AND DEFINITIONS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite has established a common set of terms and definitions for all policies, procedures, plans, and related documents.

II. Purpose

With consistent terms and definitions, F2OnSite Staff increase uniformity and understanding while reducing confusion and errors.

III. Scope

The following terms and definitions apply to all F2OnSite communications, policies, procedures, plans, and related documents.

IV. Policy

F2OnSite provides the following list of terms and definitions:

Bring Your Own Device (BYOD) – Staff owned equipment including laptops, notebooks, smartphones, tablets, and related devices.

Bring Your Own Device and Technology (BYODT) – includes both BYOD and BYOT.

Bring Your Own Technology (BYOT) – Staff owned operating systems, software applications, browsers, tools, utilities, scripts, software development kits, cloud services, and related technologies.

Certificate Authorities (CA) – sign and distribute certificates used to assure an identity when establishing encrypted communications.

Chief Security Officer (MGMT) – person responsible for information security, physical security, and security of Information Resources.

Classified Information – information that Executive Order 13526, “Classified National Security Information,” December 29, 2009 (3 CFR, 2010 Comp., p. 298), or the Atomic Energy Act of 1954, as amended, requires to have classified markings and protection against unauthorized disclosure.

Cloud Computing – the use of computing resources (e.g. hardware and software) that are delivered as a service over a network (typically the Internet).

Controlled Unclassified Information (CUI) – information (excluding Classified Information) that requires safeguarding or dissemination controls required by laws, regulations, or Government-wide policies.

Data Owner – the principal user/manager of an application or Information System.

DMZ (demilitarized zone) – a computer host or small network inserted as a "neutral zone" between a private network and an outside public network (e.g. Internet). It prevents outside users from gaining direct access to a server that has company data.

Executive Management – F2OnSite President and Vice Presidents.

Information Resources – facilities, hardware, software, Staff, and related resources.

Internet Protocol (IP) – communications protocol for routing packets across network boundaries (e.g. the Internet).

Information System – information collected, transmitted, stored, and/or archived using telephones, cell phones, pagers, voice mail, electronic mail accounts (E-mail), Internet, the World Wide Web (WWW), LAN/WAN access software, F2OnSite intranet, computers, servers, networks, peripherals, fax machines, modems, firewalls, routers, switches, hubs, and related equipment.

Information Technology (IT) – the use of computers and telecommunications equipment to store, retrieve, transmit and manipulate data.

Intranet – internal LAN used by authorized F2OnSite Staff.

LAN – Local Area Network.

Malware – malicious software including viruses, spyware, Trojan Horse programs, worms, and similar types of programs.

Personal Information – includes the following:

- Audio, electronic, visual, thermal, olfactory or similar information.

- Biometric information.
- Characteristics of protected classifications under state or federal law.
- Commercial information including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies.
- Education information, defined as information that is not publicly available personally identifiable information (PII) as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- Geolocation data.
- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, e-mail address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
- Inferences drawn from any of the information identified in this definition to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.
- Internet or other electronic network activity information including, but not limited to, browsing history, search history and information regarding a consumer's interaction with a website, application or advertisement.
- Professional or employment-related information.

Mobile Computing Device – includes laptops, notebooks, netbooks, tablets, and similar devices.

Removable Media – portable media including CDs, DVDs, memory sticks, flash drives, USB drives, portable hard drives, backup tapes, and related media.

Resource Owner – individual assigned the responsibility of granting, changing, and terminating access to an asset. Makes important decisions regarding the resource or asset.

Security Policy - the term “security policy” has several meanings. Policy can refer to F2OnSite management's directives to create an information system security program, establish its goals, and assign responsibilities. Policy can also refer to the specific security rules for particular systems. Policy may refer to specific managerial decisions such as e-mail privacy policy or password policy. Since policy may be developed and written at a broad level, all three types of policy must be supplemented with additional procedures, plans, and guidelines.

Sensitive Information – privileged or proprietary information which, if compromised through unauthorized disclosure, alteration, corruption, loss, or misuse could cause serious harm to F2OnSite.

Smartphone – a mobile phone that allows advanced computing and communications activity.

Staff – F2OnSite employees and other resources including contractors, vendors, and third-party business partners.

Tenant – a customer who uses Cloud Computing Information Resources.

WAN – Wide Area Network.

Wearable Computing Device – miniature electronic devices worn by the bearer on top of or under clothing. Examples include smartwatches, touch screens, head mounted displays, and similar devices.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff members with access to F2OnSite's Information Resources.

Policy History

Version	Date	Description	Approved By
2.0	07/01/2020	Updated Initial policy release	D Lauderback

THIRD PARTY SERVICE PROVIDERS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Third party service providers play an important role in the support of the IT infrastructure and providing information services. In some instances, service providers may collect, store, and maintain Sensitive Information. Setting limits and controls on third party service providers helps eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to F2OnSite.

II. Purpose

The purpose of this policy is to establish the rules for service provider access to company information, third party responsibilities, and protection of F2OnSite information.

III. Scope

This policy applies to all Staff responsible for the installation of new Information Resources assets, the operations and maintenance of existing Information Resources, monitoring and troubleshooting of Information Resources. It applies to third party service providers that collect, store, process, manage, and dispose of F2OnSite's information.

IV. Policy

Prior to entering into an agreement, F2OnSite Staff shall follow due diligence in selecting third party service providers. This may include background checks of service provider and related personnel, length of time in business, experience with similar engagements, etc.

Service providers must comply with all applicable F2OnSite policies, practice standards and agreements, including, but not limited to:

- Acceptable Use Policy
- Anti-Malware Policy
- Approved Application Policy
- Audit Policy
- Bring Your Own Device Policy
- Data Privacy Policy
- E-mail Policy
- Guest Access Policy
- Identification and Authentication Policy
- Network Access Policy
- Outsourcing Policy
- Password Policy
- Personnel Security Policy
- Physical Access Policy
- Physical Security Policy
- Remote Access Policy
- Removable Media Policy
- Secure Software Development Lifecycle Policy
- Security Policy
- Software Development Policy
- Staffing Policy
- User Privilege Policy
- Vendor Access Policy

As appropriate, service providers shall comply with F2OnSite's compliance related policies including, but not limited to:

- Certification and Accreditation Policy
- Compliance Policy
- Electronic Data Retention Policy
- HIPAA and HITECH Policy
- PCI Policy

F2OnSite will provide an IT point of contact for the service provider. The point of contact will work with the service provider to ensure the service provider is in compliance with the above policies.

F2OnSite IT Management shall maintain a list of all third party providers and the services performed by each. IT Management shall maintain copies of all agreements with service providers.

Agreements with third party service providers must specify:

- Confidentiality that protects F2OnSite's information as well as our customer information.
- Controlled access to F2OnSite's Information Resources.
- How F2OnSite's Information Resources are protected by the service provider.
- Acceptable methods for the return, destruction, or disposal of F2OnSite information in the service provider's possession at the end of the agreement.
- The service provider must only use F2OnSite information and Information Resources for the purpose of the business agreement.
- Any other F2OnSite information acquired by the service provider in the course of the contract cannot be used for the service provider's own purposes or divulged to others.

Each service provider must provide F2OnSite with a list of all staff working to provide services to F2OnSite. The list must be updated and provided to F2OnSite within 24 hours of staff changes.

Each on-site service provider staff member must acquire a F2OnSite identification badge that will be displayed at all times while on F2OnSite premises. The badge must be returned to F2OnSite when the service provider's employee leaves the premises.

Each service provider staff member with access to F2OnSite Sensitive Information must be cleared to handle that information. Third party access to Sensitive Information shall be activated only when needed. Access shall be deactivated after services have been provided. IDs used by vendors to access, support, or maintain system components via remote access shall only be enabled during the time period needed and disabled when not in use. Third party service provider access to Information Systems shall be monitored during use.

Service providers with remote access to customer premises (e.g. for support of Point of Sale devices or servers) must use a unique authentication credential (i.e. password/phrase) for each client.

Service provider personnel must report all security incidents directly to the appropriate F2OnSite personnel. If service provider management is involved in F2OnSite security incident management the responsibilities and details must be specified in the agreement.

Service provider must follow all applicable F2OnSite change control processes and procedures.

Regular work hours and duties will be defined in the agreement. Work outside of defined parameters must be approved in writing by appropriate F2OnSite management.

All service provider maintenance equipment on the F2OnSite network that connects to the outside world via the network, telephone line, or leased line, and all F2OnSite IT service provider accounts will remain disabled except when in use for authorized maintenance.

Service provider access must be uniquely identifiable and password management must comply with the F2OnSite Password Policy. Service provider's major work activities must be entered into the Third Party Service Provider Log Form and made available to F2OnSite management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Upon departure of a service provider staff from the agreement for any reason, the service provider will ensure that all Sensitive Information is collected and returned to F2OnSite or destroyed within 24 hours. Upon termination of service provider or at the request of F2OnSite, the service provider will return or destroy all F2OnSite information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of F2OnSite, the service provider must surrender all F2OnSite identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the service provider must be documented by authorized F2OnSite management.

Service providers are required to comply with all State and F2OnSite auditing requirements, including the auditing of the service provider's work.

All software used by the service provider in providing service to F2OnSite must be properly inventoried and licensed.

Agreements with third party service providers shall include explicit coverage of all relevant security requirements. Agreements shall include controls over the processing, accessing, communicating, hosting or managing the organization's Information Resources or adding or terminating services or products to existing information. Agreements shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

Agreements with third party service providers shall require the provider to acknowledge that they are responsible for the security of F2OnSite sensitive information the service provider possesses or otherwise stores, processes, or transmits on behalf of F2OnSite to the extent that they could impact the security of the data environment.

Agreements with third party service providers shall specify that the third party service provider will notify F2OnSite within five (5) working days of discovery of a service provider security breach. Upon such notification, F2OnSite shall have the right, but not the obligation, to terminate the agreement with the service provider. If the service provider had access to F2OnSite customer information, the service provider shall pay for all costs incurred to remedy the breach including, if appropriate, notifying F2OnSite's customers, paying for one year of free credit report for F2OnSite's customers, and related expenses.

When dealing with health information, service providers shall provide an on-line and print description of security and privacy directives, guidelines, policies, and security safeguards that protect Sensitive Information.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for the installation of new Information Resources assets, the operations and maintenance of existing Information Resources, monitoring and troubleshooting of Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback

References:

COBIT APO09.05, APO10.05, APO12.02, APO13.07, BAI02.05-06, DSS01.05, DSS05.07
GDPR Article 25, 26, 28, 32
HIPAA 164.308(a)(1)(ii)(A), 164.308(b)(4), 164.502(b)(1), ARRA 13404(b), ARRA 13405(b)
ISO 27001:2013 8.1, A.13.1.2, A.14.2.7
NIST SP 800-37 3.3, 3.7
NIST SP 800-53 PS-7, RA-9, SA-4, SA-10-12, SA-15, SA-17
NIST Cybersecurity Framework ID.AM-4-6, ID.BE-4, ID.RA-4, ID.RM-1, ID.SC-3-4, DE.CM-6
PCI 12.8, PCI Software Security Framework

USER PRIVILEGE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

This policy defines the privileges various users on the organizational network are allowed to have, specifically defining what groups of users have privileges to install computer programs on their own or other systems. This policy defines the users who have access to and control of sensitive or regulated data. This policy defines Internet access to specific sites for some users or other ways they may or may not use their computer systems.

II. Purpose

This policy is designed to minimize risk to organizational resources and data by establishing the privileges of users of data and equipment on the network to the minimum allowable while still allowing users to perform job functions without undue inconvenience.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

A. Types of users

Main categories of users on a computer or network include:

- Restricted user – can operate the computer and save documents but can't save system settings.
- Standard user (power user) – can change many system settings and install programs that don't affect Windows system files.
- Administrators – have complete access to read and write any data on the system and add or remove any programs or change system settings. The majority of users on most common networks should be restricted users on their local computers.

Only users with special training or a need for additional access should be allowed to change system settings and install programs that are not operating system programs. This is because many viruses and adware or spyware may be installed in a subtle manner by tricking the user or the installation may be completely transparent to the computer user. If the user does not have the ability to install programs or change settings to a more vulnerable setting, most of these potential security problems can be prevented. Therefore only users that demonstrate a need and ability for power user or administrator access on local machines shall be permitted to have this level of access. Upon demonstration of a special need for additional access, the IT Director must approve the access before it can be made effective. Examples of users with special privileges include domain administrators, help desk personnel, and application developers.

B. Network resources

Most network users will have access to the following types of network resources.

- E-mail – most users will have full access to their own e-mail. They will not be able to transfer ownership to someone else.
- A mapped drive on a networked file server – a folder on a drive that only the primary user of this drive can read and write exclusive of domain administrators. The user will not be able to transfer ownership to someone else.
- A shared group or organizational division's drive – a folder that members of specific groups or divisions in the organization may access. Access may be read or write and may vary by organizational requirements.
- Access to databases – databases stored on a shared drive or other resource. Most databases will have a standard user level which gives users appropriate permissions to enter data and to see report information. However only the database administrators shall have full access to all resources on a database. Database administrators will only have full access to the database that they administer.

Groups that may be allowed additional access include:

- Backup operator – allowed to read data on the domain for the purpose of saving files to backup media. This group cannot write all data on the domain.
- Account operator – can manage and view information about user accounts on the domain.
- Server operator – has full privileges on servers including reading and writing of data, installing programs, and changing settings.

- Domain administrator – has full privileges on all computers in the domain including servers and workstations. Privileges include reading and writing data, installing programs, and changing settings.

C. Security Considerations

The Chief Security Officer shall ensure:

- The organization shall implement administrative, physical, and technical safeguards to protect sensitive information confidentiality, integrity, and availability. The organization shall ensure that any agent, including a subcontractor, agrees to implement reasonable and appropriate safeguards.
- Electronic mechanisms corroborate that sensitive information has not been altered or destroyed in an unauthorized manner. Information Systems that contain sensitive information shall automatically check for data integrity (e.g. check sums verification, digital signature).
- Third party service providers and business associates (e.g. billing services, hardware and software vendors, external consultants, lawyers) have been identified. The organization has established written contracts or other arrangements with business contacts and third party service providers that meet security requirements. Contracts are in place with third party service providers to ensure security requirements are addressed. Before sensitive information is disclosed, the organization shall receive assurances from third party service providers and each associate that they appropriately safeguard information. Refer to the Third Party Service Providers Policy for more information.
- The organization shall be provided with a report if the third party service provider or business associate experiences a security incident. Procedures shall specify the process to terminate the contract with the third party service provider or business associate if they have violated a material term of the contract or experienced a material breach.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT APO01.02, APO01.11, APO14.10, BAI09.03-04, DSS01.05, MEA02.11
 GDPR Article 25, 32
 HIPAA 164.308(a)(3)(ii)(A), 64.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.310(b)
 ISO 27001:2013 5.3, 6.1.3, A.6.1.2, A.7.2.1, A.8.1.3, A.9.1.2, A.9.2.2-3, A.9.4.1, A.9.4.4
 NIST SP 800-37 3.3, 3.6, 3.7
 NIST SP 800-53 AC-2-3, AC-5-6, AC-24, CM-5, PL-4, PS-6, PS-7, SA-9
 NIST Cybersecurity Framework PR.AC-1, PR.AC-4, PR.AT-2, DE.CM-1-3, DE.DP-2, RS.RP-1
 PCI 7.1-2, 8.1, 10.2, A1.1-2, A3.4.1

VENDOR ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to F2OnSite.

II. Purpose

This policy establishes the rules for vendor access to F2OnSite's Information Resources and support services, vendor responsibilities, and protection of F2OnSite information.

III. Scope

This policy applies to all Staff that use F2OnSite Information Resources.

IV. Policy

Vendors must comply with all applicable F2OnSite policies, procedures, and agreements including, but not limited to:

- Safety policies
- Privacy policies
- Security policies
- Auditing policies
- Software licensing policies
- Acceptable use policies

The IT Department shall implement and maintain a consolidated list of vendors with access to F2OnSite's Information Resources. Such list, as well as vendor agreements and contracts, must specify:

- The F2OnSite resources the vendor to which the vendor has access.
- How F2OnSite information is to be protected by the vendor.
- Acceptable methods for the return, destruction, or disposal of F2OnSite information in the vendor's possession at the end of the contract.
- The vendor must only use F2OnSite information and Information Resources for the purpose of the business agreement.
- Any other F2OnSite information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

F2OnSite will provide a point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with F2OnSite policies.

Each vendor must provide F2OnSite with a list of all Staff working on the contract. The list must be updated and provided to F2OnSite within 24 hours of staff changes.

Each on-site vendor employee must acquire an F2OnSite identification badge that will be displayed at all times while on F2OnSite premises. The badge must be returned to F2OnSite when the employee leaves the contract or at the end of the contract.

Each vendor employee with access to F2OnSite sensitive information must be cleared to handle that information.

Vendor personnel must report all security incidents directly to the appropriate F2OnSite personnel. If vendor management is involved in F2OnSite security incident management the responsibilities and details must be specified in the contract.

Vendor must follow all applicable F2OnSite change control processes and procedures.

Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate F2OnSite management.

All vendor maintenance equipment on the F2OnSite network that connects to the outside world via the network, telephone line, or leased line, and all F2OnSite IT vendor accounts will remain disabled except when in use for authorized maintenance.

Vendor access must be uniquely identifiable and password management must comply with the F2OnSite Password Policy. Vendor's major work activities must be entered into the Third Party Service Provider Log Form and available to F2OnSite management upon request. Log entries must include, but are not limited to, such events as

personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to F2OnSite or destroyed within 24 hours.

Upon termination of contract or at the request of F2OnSite, the vendor will return or destroy all F2OnSite information and provide written certification of that return or destruction within 24 hours.

Upon termination of contract or at the request of F2OnSite, the vendor must surrender all F2OnSite identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized F2OnSite management.

Vendors are required to comply with all State and F2OnSite auditing requirements, including the auditing of the vendor's work.

All software used by the vendor in providing service to F2OnSite must be properly inventoried and licensed.

Third party agreements that directly, or indirectly, impact Information Resources are required to include explicit coverage of all relevant security requirements. This includes agreements involving processing, accessing, communicating, hosting or managing the organization's information assets, or adding or terminating services or products to existing information. Asset agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT APO09.05, APO10.05, APO12.02, APO13.07, BAI02.05-06, DSS01.05, DSS05.07
GDPR Article 25, 32
HIPAA 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(b)(4)
ISO 27001:2013 8.3, A.5.1.1, A.9.2.6, A.11.1.2, A.13.2
NIST SP 800-37 3.3, 3.6, 3.7
NIST SP 800-53 AC-2, AC-21, CA-3, PA-4, PE-2-5, PS-4-6, SA-9
NIST Cybersecurity Framework ID.AM-4-6, ID.RA-4, ID.RM-1, ID.SC-2-4, PR.AT-3, DE.CM-6
PCI 2.5, 7.1-3, 8.1-2, 8.5-6, 8.8, 9.1-4

VIRTUAL PRIVATE NETWORK (VPN) POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

This policy provides guidelines for remote access connections to F2OnSite's Information Systems, if implemented by the Company

II. Purpose

This policy is established to help protect the integrity, availability and confidentiality of information, to prevent loss of service, and to comply with legal requirements.

III. Scope

This policy applies to all Staff that administer, monitor, maintain, or remotely use F2OnSite's Information Systems.

IV. Policy

Approved F2OnSite Staff may remotely connect to Company's Information Systems. Virtual Private Network (VPN) technology provides an encrypted tunnel so that information transmitted to and from Company's systems are not easily readable by unauthorized parties.

F2OnSite Staff are responsible for selecting and providing an Internet Service Provider (ISP), coordinating the installation of Company approved VPN software through the IT Department, installing any required software, and paying associated fees.

It is the responsibility of Staff with VPN privileges to ensure that unauthorized users are not allowed access to F2OnSite internal networks from the Staff member's remote location.

IT Staff shall ensure that VPN use is controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong passphrase.

When actively connected to F2OnSite's Information Systems, IT Staff shall ensure that implementations force all traffic to and from the user workstation through the VPN tunnel. All other traffic shall be dropped.

Dual (split) tunneling is NOT permitted and only one network connection is allowed. VPN gateways shall be set up and managed by F2OnSite's IT Department.

All computers connected to F2OnSite's Information Systems via VPN or any other similar remote technology must use up-to-date anti-malware software as stated in F2OnSite's Anti-Malware Policy.

VPN users shall be automatically disconnected from F2OnSite's Information Systems network after a period of inactivity. The VPN user must then logon again to reconnect to the network. Pings or other artificial network processes shall not be used to keep the connection open.

Users of computers that are not F2OnSite owned equipment must configure the equipment to comply with F2OnSite's policies. By using VPN technology with personal equipment, VPN users must understand that their machines are an extension of F2OnSite's network, and as such are subject to the same rules and regulations that apply to F2OnSite owned equipment.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT APO12.02, APO12.07, APO14.07, BAI02.05, BAI10.07, DSS01.05, DSS05.07, DSS06.08

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.312(a)(2)(iv), 164.312(d), 164.312(e)(2)(ii)

ISO 27001:2013 8.3, 9.1, A.6.2.2, A.8.1.3, A.9.1.2, A.9.2.2-3

NIST SP 800-37 3.3, 3.7

NIST SP 800-53 AC-2-3, AC-6, AC-17, CM-5, PE-17, PL-4

NIST Cybersecurity Framework PR.AC-3, DE.CM-1, DE.DP-2

PCI 2.3, 7.1-3, 8.1.5

VULNERABILITY AND PENETRATION TESTING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Vulnerability assessments and penetration tests evaluate systems for security related vulnerabilities.

II. Purpose

Vulnerability assessments and penetration tests help ensure that security controls are sufficient and effective at providing information confidentiality, availability, and integrity.

III. Scope

This policy applies to all Staff responsible for the installation and support of IT, individuals charged with IT Security, data owners, Chief Executive Officer (CEO), and President

IV. Policy

Vulnerability assessments and penetration tests identify and help reduce risks to F2OnSite's Information Systems.

- Vulnerability assessments search Information Systems for known vulnerabilities. Examples include patches that haven't been installed, weak encryption, etc.
- Penetration tests attempt to actively exploit weaknesses in an environment. Examples include SQL injection attacks, cross site scripting, etc. Penetration tests can also include social engineering to evaluate the effectiveness of Staff security education and awareness training.

The CEO responsible for ensuring that security controls and safeguards are appropriate, sufficient, and effective at treating risks. The CEO shall:

- Evaluation – identify the type of evaluation(s) to be performed. These include vulnerability assessment, penetration test, or both vulnerability assessment and penetration test.

- Scope – define the scope including systems being evaluated, timeframes, controls to be used, etc. Determine if social engineering is included in the scope.
- Resources – identify resources to perform the evaluation.

Access to vulnerability assessment and penetration testing tools shall be controlled and restricted to prevent possible misuse or compromise of Information Resources and log data. The evaluation shall be carefully planned and agreed to minimize disruptions to business processes.

The CEO shall develop and maintain a program for penetration testing that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks. Such test program shall consider a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production. These include attacks against supervisory control, data acquisition, and other control systems.

Where possible, IT security Staff shall utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify potential vulnerabilities on the organization's systems.

The CEO shall use Certified Information Systems Auditors to perform an independent evaluation. Evaluations shall be performed on an annual basis or more frequently if major changes occur to Information Resources or Staff. The report deliverable shall identify the project scope, findings, and recommendations to enhance security. The CEO shall:

- Review the report to confirm the findings and verify the security recommendations are sufficient and effective.
- Convey the findings to the Risk Management Officer and appropriate Department Heads so that a Risk Treatment Plan and Risk Task List can be prepared or updated as necessary.

The CEO shall document important findings in the Audit Log Form and The Risk Management Officer shall provide necessary reporting to F2OnSite Executive Management.

V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Department Heads, Chief Security Officer, Risk Management Officer, and those responsible for information system security.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT EDM03.07, APO12.02, APO12.07, APO13.07, BAI10.07, DSS05.07, MEA01.05
GDPR Article 32
HIPAA 164.308(a)(8)
ISO 27001 9.2, A.15.2.1
NIST SP 800-37 3.5
NIST SP 800-53 3.3, AC-5, AU-6, CA-2
NIST Cybersecurity Framework ID.SC-4, PR.AC-1, PR.PT-1, DE.CM-8, DE.DP-2
PCI 2.2.a-d, PCI Software Security Framework

WEARABLE COMPUTING DEVICE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Today's Wearable Computing Devices include advanced features such as the ability to connect to the Internet, run applications, take videos, use wireless connectivity, etc. While Wearable Computing Devices increase productivity, they also come with risks.

II. Purpose

The purpose of this policy is to help manage Wearable Computing Device related risks Staff members and F2OnSite.

III. Scope

This policy applies to all F2OnSite Staff that use Information Resources.

IV. Policy

Only IT Department approved Wearable Computing Devices may be used to access F2OnSite networks and Information Resources.

F2OnSite uses a multi-layered approach to protecting Wearable Computing Devices and related "information assets". Securing Wearable Computing Devices is the responsibility of both the device user as well as F2OnSite's IT Department.

User activities can download malware to a Wearable Computing Device. Once installed, the malware can launch attacks against F2OnSite's internal network. Staff security education and awareness training should be provided on a regular basis. Staff should only download and install applications from trusted sources. In addition, Staff should not click on message links from unknown senders or visit unknown web sites.

If possible, Wearable Computing Device protection software should be installed on all devices that access the Internet and especially Wearable Computing Devices that access F2OnSite's Information Systems.

F2OnSite's IT Department shall establish standards for Wearable Computing Devices, phone protection software, etc. This reduces IT administration costs and offers better protection for the enterprise.

Wearable Computing Devices shall have security mechanisms that protect against unauthorized access to F2OnSite's Information Systems. Examples include passwords and devices equipped with sensors that read the electrocardiogram (ECG) of the person wearing the device to validate the person's own unique heartbeat signature prior to granting access to Information Resources.

The F2OnSite IT Department shall perform periodic risk assessments to identify, manage, and reduce Wearable Computing Device related risks and access to Information Resources. Refer to the Risk Assessment Policy for more information.

The IT Department shall implement procedures and measures to strictly limit access to sensitive data from Wearable Computing Devices which are generally higher-risk than non-portable devices (e.g., desktop computers).

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2OnSite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT APO10.05, APO12.02, APO13.07, BAI02.05, BAI03.05, DSS01.05, DSS05.02
GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(A), 64.308(a)(4)(ii)(B), 164.310(b), 164.310(c)

ISO 27001:2013 8.2, A.6.2

NIST SP 800-37 3.1, 3.3

NIST SP 800-53 AC-19, AC-20, AU-6, CA-9, CM-8, MP-6, MP-7, SA-18, SC-8, SC-42, SC-43

NIST Cybersecurity Framework ID.AM-1, ID.GV-4, ID.RA-4, PR.AC-1-4, PR.AT-1, DE.DP-2

PCI 1.1.5, 1.1.6, 1.2.1, 1.2.3, 1.4, 2.2

WEB SITE POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

F2OnSite's web site is used to convey information to prospects, customers, staff, suppliers, and other business contacts. Our web site is important to our organization's image and reputation.

II. Purpose

This policy helps provide a consistent look and feel for F2OnSite's web site. In addition, it helps protect F2OnSite's image and reputation.

III. Scope

This policy applies to all Staff who develop, program, provide content for, and otherwise maintain the F2OnSite's web site.

IV. Policy

Design of web sites must comply with F2OnSite's standards. Any F2OnSite web site designed by any person or vendor other than F2OnSite's IT Department must be submitted to the Marketing Department for review and approval.

Every page of the site must contain the F2OnSite logo in a prominent location near the top of the page. The F2OnSite logo must link to F2OnSite's home page. The primary colors of the site must be black (#000000) and white (#ffffff).

At minimum, the design must seek to make essential information and functions available to all users. The pages must function:

- Display properly in popular browsers including Internet Explorer.
- Function on both Windows and Macintosh operating systems.

- Open documents (e.g. pdf, Word.) in a new Window without generating error messages.
- If required, provide a link for the visitor to download required plug-ins.

Contact information should be identified on the appropriate pages. The main page of the web site shall provide links to other areas of the site. The Contact Us page shall include F2OnSite's address, telephone, and e-mail information.

Many publications, photos, and art work are protected by copyright law. All federal copyright and trademark rules and regulations must be observed. The web site shall provide the following copyright statement on the Company web site: Copyright © F2OnSite (year).

The Home page shall include a link to F2OnSite's Web Site Privacy Policy. The text link or button shall be of the same size and color as other links on the home page. The Web Site Privacy Policy shall include:

- Notice – personal information collected on the site
- Choice – options the visitor has about how personal data is collected and used
- Access – data this is collected and how a visitor can make changes to their information
- Security – steps taken to protect data that is collected and stored
- Remedy – steps the visitor can take if the Website Privacy Policy is not met

F2OnSite does not permit outside advertisements to be placed on our web site. This includes links, logos, or other identifiers that promote, induce or encourage, directly or indirectly, commercial activity of any sort with or for the benefit of any person or entity other than the F2OnSite, or that endorses or recommends directly or indirectly the products, facilities or services of any person or entity.

Secure areas of the web site shall be protected by appropriate security measures including access controls and encryption. See the Access Control Policy and Encryption Policy for more information.

The web site shall be patched and updated in a timely manner per the Patch Management Policy.

Periodic web site security audits shall be performed per the Audit Policy.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for managing and developing the F2OnSite web site.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT EDM01.01, APO01.03, APO01.11, APO05.03, APO12.02, APO13.07, MEA04.11
 GDPR Article 25, 32
 HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(8)
 ISO 27001:2013 8.3, A.10.1, A.12.6, A.14.1, A.18.2.1
 NIST SP 800-37 3.4, 3.4
 NIST SP 800-53 CA-2(1), CA-7(1), RA-3, RA-5, SA-3-4, SA-11(3), SC-12-13, SC-17, SI-2, SI-5
 NIST Cybersecurity Framework ID.AM-2, ID.AM-4, ID.GV-4, ID.RA-6, ID.RM-1, PR.AC-3-4
 PCI 4.1, 6.1, 6.5, 11.2.2

WEB SITE PRIVACY POLICY

Policy Area	IT Policy Library
Approved Date	December 31, 20XX
Approved By	Policy Committee
Effective Date	January 1, 20XX
Current Version	1.0

I. Overview

F2OnSite's Web Site Privacy Policy discloses to web site visitors the ways F2OnSite collects, uses, discloses, and protects visitor data.

II. Purpose

F2OnSite provides this Web Site Privacy Policy to provide transparency to web site visitors and meet compliance and privacy requirements. We believe that providing visitors with accurate and adequate notice about our web sites will lead to informed choices and decisions about how to use web sites as well as protect visitor privacy.

III. Scope

This policy applies to all Staff who manage, develop, program, provide content for, and otherwise maintain the F2OnSite's web site.

IV. Policy

A. Overview

Web sites must comply with F2OnSite's Web Site Policy. Web site designs must comply with F2OnSite's standards. Any F2OnSite web site designed by any person or vendor other than F2OnSite's IT Department must be submitted to the Marketing Department for review and approval.

Recommended web site privacy policy content is listed below. However, the content may be changed:

- To customize the content regarding F2OnSite's products and services.
- As new services are provided.
- To meet regulatory compliance and best practice requirements.

- To provide additional transparency on personal information collected, stored, and protected.

B. Recommended Web Site Privacy Policy Content

Web Site Privacy Policy

F2OnSite is committed to protecting your privacy. Most pages on our site can be visited without providing information about yourself or your organization. Occasionally, we need your contact information to provide services that you request. This Privacy Policy explains our data collection procedures and use of your information. This notice informs you about:

- Your privacy rights
- Personal information that may be collected.
- Access to your personal information.
- How your information may be used, including, with whom, if anyone, it might be shared.
- Choices you have regarding the use of your personal information.
- How we safeguard your information.
- How you can access and, if necessary, change or delete your personal information.
- Please contact us [[Link to Contact us page on web site](#)] if you have any questions, complaints, or comments regarding this Privacy Policy.

When you link to any other site, you leave F2OnSite's site and we have no control over the activities or policies of other sites.

Our Do Not Sell My Personal Information [[Link to Do Not Sell page on web site](#)] page provides more information. Individuals receive equal service and price and are not discriminated against for exercising their privacy rights.

Your Privacy Rights

F2OnSite respects your privacy rights:

- Right to Know. You have the right to know when we intend to collect personal information, what personal information is being or has been collected, where the data originated, how it will be used, and with whom it will be shared.
- Right to Consent. You have the right to opt-in for the use, disclosure, sale, or access to your personal information. You may revoke such consent at any time.
- Right to Prevent. You have the right to prevent our organization from sharing your personal information with third parties.
- Right to Request. You have the right to request a copy of your personal information on file.
- Right to Deletion. You have the right to request that we remove your personal information on file.
- Right to Pricing. We are prohibited from charging you a different price, or refusing service, if you exercised your privacy rights.

Personal Information Collected

Contact information collected is generally limited to your name, organization name (if applies), address, phone number, and e-mail address. Information is requested when you request or register to receive more information, subscribe to e-mail newsletters, sign up for an event or training, or order services.

F2OnSite may request and/or collect additional information from you on a voluntary basis when you:

- Request information on or purchase our products or services.
- Participate in promotions or events.
- Send questions or comments via e-mail to F2OnSite.

When you send e-mail to us, we are not attempting to collect any personal information about you. We will only use information contained in your e-mail to respond to your specific inquiry or comments in the e-mail. Since e-mail is a form of business communication, we may retain your information for a period of time and archive such information per F2OnSite's retention requirements.

This site collects information about pages visited within the site. We may use this information to accurately count visitors across our web sites and understand how they navigate and use our network of web sites. F2OnSite does not combine web site traffic information with your personal information.

F2OnSite does not:

- Share your information with unaffiliated third parties for their own direct marketing purposes.
- Knowingly collect personal information on European Union (EU) residents.
- Collect, transmit, or store, personal information such as medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex of the individual.

How Personal Data is Used

F2OnSite collects, stores, and processes information provided to us. We may use the information you submit to us to send you information on our products, services, and promotional materials. Specifically, we use your contact information for the following purposes:

- Respond to your specific inquiry or comments.
- Deliver services, including marketing communications, related to your request or use of our products and services.

- Alert you to special offers, updated information, new services, and related information from F2OnSite.
- Allow you access to limited-entry areas of our site as appropriate.
- Other forms of business correspondence.

Purchases made via the web site may capture your name, address, phone number, e-mail address, and payment information (e.g. credit/debit card, PayPal, etc.). F2OnSite uses a third party merchant for payment transactions.

We may use your information so we can improve the products and services we provide to better meet your needs. The demographic information (e.g., location, type of organization, services requested, etc.) you provide us is collected by F2OnSite and is not disclosed to third parties. This demographic information cannot be used to personally identify you. We may merge site-visitation data with anonymous demographic information for research purposes, and we may use this information in aggregate to provide more relevant content.

F2OnSite reserves the right to use "cookies" to enhance your experience at our web site. Cookies are pieces of information that we place on your computer to help us accurately understand how many visitors are viewing a particular site, how often they visit that site, and the content viewed. F2OnSite reserves the right to collect IP addresses for the purposes of system administration, to report aggregate information to third party marketing firms, and to audit the use of our web sites. When visitors request pages on our web site, our servers may log the visitor's IP address. We do not link the IP address to your personally identifiable information.

Information passively collected by F2OnSite includes log files that record web site activity that gathers statistics about web user browsing habits. These entries are generated anonymously, and help F2OnSite determine, among other things, how many and how often users visit our web site, the pages visited, and other similar data. We also use the log file entries for internal marketing and demographic studies to constantly improve our online services.

Sharing of Information

F2OnSite may share your personal information with outside entities hired to assist with F2OnSite's internal support operations (e.g. cloud service providers, packaging and mailing services, event registration, etc.). We only provide those companies the information they need to deliver the service, and they are prohibited from using that information for any other purpose. Third parties may also collect your personal information from other sources.

F2OnSite does not sell or rent information collected from and about individuals to third parties. In the past 12 months, we have not sold or rented individual personal

information to third parties. However, in the event of a merger, acquisition, reorganization, bankruptcy, or other similar event, your personal information may be transferred to F2OnSite's successor or assign, if permitted by and done in accordance with applicable law.

F2OnSite may disclose your contact information if required to do so by law or in the good-faith belief that such action is necessary to:

- Conform to the edicts of the law including disclosure of information in response to lawful requests by public authorities, national security or law enforcement requests, or comply with legal process served on F2OnSite.
- Protect and defend the rights or property of F2OnSite and its web site.
- Investigations of fraud, intellectual property right infringements, or other activity that is illegal.
- Act in urgent circumstances to protect the personal safety of F2OnSite employees, users of F2OnSite products or services, or members of the public.

Safeguarding Information

F2OnSite only collects information to the extent deemed reasonably necessary to serve our legitimate business purposes. In addition, we take appropriate steps to ensure the security and integrity of any information you provide to us.

Any information provided to us is stored in an access-controlled facility. Your information is protected from electronic threats by the use of firewalls, intrusion detection, anti-virus, anti-spyware, passwords, and related security mechanisms.

Update and Removal of Information

If you receive an e-mail and want to opt-out, simply reply back to the e-mail requesting your address be removed from future communications or click the unsubscribe link, if provided.

You may at any time review, correct, amend, or delete the contact information we have for you. Simply contact us [[Link to Contact us page on web site](#)] to change, update, or have us remove your information. If your request is sent via e-mail, please include in your message the service or communication you received from us.

Age Notice

F2OnSite has developed this web site to be an enjoyable experience for visitors of all ages. F2OnSite recognizes that some younger children may not understand some of the information contained on the web site or how the web site operates.

Most areas of this site are available to the general public, including those under the age of 13.

Children under the age of 13 should seek parent or guardian's consent before they provide any personal information to us.

Adults should monitor and restrict the activities of their children. In addition, F2OnSite requests that adults discuss this Privacy Policy with your children so that they will better understand how to use this web site and the information they may be asked to provide.

Inquiries, Comments, or Complaints

Please submit any questions, comments, inquiries, or complaints to F2OnSite using the contact us [[Link to Contact us page on web site](#)] page on our web site.

Effective Date and Changes to Privacy Policy

This Privacy Policy is effective as of January 2, 20XX. You will be notified by prominent notice on this page if there are material changes to this Privacy Policy.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Staff responsible for managing and developing the F2OnSite web site.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Updated Initial policy release	D Lauderback
2.1	07/07/2020	Reviewed	J Poole

References:

COBIT EDM01.01, APO01.03, APO01.11, APO05.03, APO12.02, APO13.07, MEA04.11
GDPR Article 24, 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.502(b)(1), ARRA 13404(b), ARRA 13405(a)
ISO 27001:2013 A.9.1.1, A.9.2.2, A.18.1.3-4
NIST SP 800-37 3.2, 3.4, 3.7
NIST SP 800-53 AC-3-4, AC-6, AC-21, AC-23, AU-9-10, Appendix F, Table F-1
NIST Cybersecurity Framework ID.AM-3, ID.GV-3, ID.RM-1, PR.AC-1-4, PR.AC-6, DE.DP-2
PCI 8.6, 9.1-4, 9.9

WIRELESS ACCESS POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Staff shall use the proper security controls when using wireless devices to connect to F2Onsite's Information Systems.

II. Purpose

F2Onsite has developed a set of standards for the use and deployment of Wireless networks.

III. Scope

This policy applies to all Staff that use and deploy wireless networks.

IV. Policy

A. Introduction

This policy provides guidance to F2Onsite System Administrators who deploy and manage wireless networks as well as to Staff who use wireless networks. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media. The use of wireless connectivity for enterprise applications is not recommended.

By using personally owned devices within the F2Onsite network for business purposes, Staff members are subject to F2Onsite policies restricting their use. Any personally owned devices, such as Smartphones, Wearable Computing Devices, wireless devices, or other electronic transmitters determined to have contributed to a security incident may be subject to seizure and retention by F2Onsite Staff.

B. Connectivity Considerations

Wireless networks are limited in speed, bandwidth, and coverage. Where possible, the use of a wired connection is preferred because it is faster and it does not compete with other wireless stations (clients) for bandwidth.

Weak signal strength can lead to reduced Staff productivity. The IT Department will perform a general site survey to determine the best placement strategies for wireless access points.

To reduce risks related to wireless networks

- Wireless networks shall not be connected to F2Onsite's internal network (LAN).
- Users inside the F2Onsite firewall may not connect to the F2Onsite network if they are using a wireless connection to connect to an external network.
- Wireless access points or devices with wireless capability are not allowed unless approved by the IT Department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to F2Onsite's internal network.

Wireless security best practices shall be implemented and include:

- Logical and physical user access to wireless network devices restricted to authorized personnel and devices.
- Perimeter firewalls shall be implemented and configured by IT security Staff to restrict unauthorized traffic.
- Vendor default settings (e.g. passwords, wireless encryption keys, SNMP community strings) are changed prior to installing wireless equipment in a production environment.
- Wireless security practices ensure security and include highest encryption possible, disabling of SSID, and strong passwords changed on a periodic basis.
- IT security Staff testing for the presence of ad-hoc wireless access points on a quarterly basis. Any findings, evidence, and actions taken should be documented and retained per F2Onsite's Data Retention Policy.

Network diagram(s) shall identify connections between internal networks and wireless networks.

C. Security

Wireless (Wi-Fi) transmissions that are used to access F2Onsite mobile computing devices or wireless networks must be encrypted. If sent across the Internet (e.g. external to F2Onsite's network) or other open networks such as wireless connections, both the authentication data (e.g. a user ID and password) and the data itself must be encrypted with strong encryption. Data must not be transmitted via wireless to or from a

portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.

The Chief Security Officer shall ensure:

- Sensitive information is encrypted using the strongest and most cost effective encryption available.
- Wireless networks transmitting sensitive data or connected to sensitive data environments shall use industry best practices (e.g., IEEE 802.11i or Advanced Encryption Standard) to implement strong encryption for authentication and transmission.
- A separate wireless network shall exist for personal or untrusted devices. Access to the internal network from this network should be treated as untrusted, filtered, and audited accordingly.
- Processes test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.
- Procedures maintain an inventory of authorized wireless access points including a documented business justification.
- Incident response procedures are implemented in the event unauthorized wireless access points are detected.
- Older encryption protocols such as Wired Equivalent Privacy (WEP) or SSL are not used for authentication or transmission.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2Onsite Staff.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D LAUDERBACK

References:

COBIT APO01.03, APO03.06, APO12.02, APO13.07, BAI02.05, BAI10.07, DSS01.05, DSS05.07

GDPR Article 25, 32

HIPAA 164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B), 164.310(c)

ISO 27001:2013 8.3, A.6.2, A.8.1.3, A.9.1.2, A.9.4.1, A.10.1.1, A.13.1

NIST SP 800-37

NIST SP 800-53 AC-2-4, AC-6, AC-17-18, AC-24, CA-3, PE-17, PL-4, SA-9, SC-7,-8, SC-10

NIST Cybersecurity Framework PR.AC-3-4, PR.AT-1, PR.DS-2, DE.CM-1, RS.RP-1

PCI 1.1.2, 1.2.3, 2.1.1, 4.1, 9.1.3, 11.1, 12.3, 12.10.3

WORKSTATION HARDENING POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Workstations are used by F2Onsite Staff to accomplish their day-to-day duties. Workstations must be protected from both security and performance related risks. One of the required steps to attain this assurance is to ensure that the workstations are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

II. Purpose

The purpose of this policy is to provide guidance and define the requirements for installing a new workstation in a secure manner and maintaining the security integrity of the workstation and application software.

III. Scope

This policy applies to all Staff that use and manage F2Onsite workstations.

IV. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of information. This Policy helps ensure that access to sensitive information is restricted to authorized users.

A Workstation Hardening Procedure shall provide the detailed information required to harden F2Onsite workstations. At a minimum, the Server Hardening Procedure shall include:

- Installing the operating system from an IT approved source
- Applying vendor supplied patches
- Removing unnecessary software, system services, and drivers
- Setting security parameters including workstation firewall and password at start-up

- Systems shall have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected
- Workstations shall be protected by current and up-to-date anti-malware software and definitions

Workstations shall have vendor-issued critical security updates and patches installed in a timely manner (typically within 30 days). Refer to the Patch Management Policy for more information.

Where practical, F2Onsite's IT Department will test security patches against IT core resources before installing in production environments and rolling out to user workstations.

In the case of special applications, F2Onsite's IT Department may make hardware resources available for testing security patches.

All sensitive information must be stored on network servers. Sensitive information shall be encrypted and comply with F2Onsite's Encryption Policy. Laptops containing sensitive information shall have the hard drives encrypted and laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2Onsite Staff that use Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D LAUDERBACK

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)
ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14
NIST SP 800-37 3.3, 3.4
NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10
NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1
PCI 2.1-3, 2.5-6, 4.1, 5.1

WORKSTATION HARDENING PROCEDURE

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

Policies provide management direction and guidance to ensure systems and data are properly protected. Procedures document a detailed description of the steps necessary to perform specific operations that comply with F2Onsite's policies.

II. Purpose

The purpose of this procedure is to formally document the series of steps taken to meet the requirements specified in F2Onsite's Workstation Hardening Policy.

III. Scope

This procedure applies to IT Department Staff who administer workstations.

IV. Procedure

Physical security. Ensure workstations are placed in physical locations that restrict access to authorized individuals. Laptops and other mobile devices shall be secured through the use of cable locks or locking the devices in drawers or cabinets when not in use.

Accounts. Delete unneeded user accounts.

Applications. Remove unneeded programs, applications, and services.

Alerts, advisories, and vulnerability announcements. Monitor manufacturer alerts, advisories, and vulnerability announcements. Ensure patches and updates are installed at the time a new workstation is placed into production and on-going per the Patch Management Policy.

Passwords. Educate users to choose a long and complex memorized secret (i.e. password) that complies with the Password Policy. When changing a password, educate users not to choose a recent prior password (password history). See the Password Policy for more information.

Groups. Where possible, assign the user/account to a group. Review and maintain group access rights on a regular basis.

Firewall. As a general rule, each workstation should have a software firewall activated on the device. The software firewall helps protect against network based attacks.

Anti-Malware. Ensure the device is protected from malicious software such as viruses, worms, Trojan Horse programs, etc. Ensure the Malware software and definitions are updated in a timely manner. Refer to the Anti-Malware Policy for more information.

Sharing. Where possible, disable file and printer sharing services.

Monitors. Configure workstations to have a password protected screen saver activated within a short timeout period. This ensures that workstations that were left unsecured are protected. Position monitors so that only authorized personnel can read the information on the screen.

Data. Where possible, configure the Workstation so all Sensitive Information is stored on network servers. Sensitive Information shall be encrypted and comply with F2Onsite's Encryption Policy. Laptops containing Sensitive Information shall have the hard drives encrypted.

Testing. Where possible, the device should be tested prior to installing the device in a production environment.

Management sessions. Administrators should not connect to the device using unsecure services where communications are not encrypted. Ensure only authorized personnel are allowed to access and administer the device.

Manufacturer resources. Refer to manufacturer resources for additional guidance on hardening workstations and specific security functionality.

V. Enforcement

Any Staff member found to have violated this procedure may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to IT Department Staff who administer workstations and the Chief Security Officer.

Procedure History

Version	Date	Description	Approved By
2.1	07/07/2020	Initial procedure release	D LAUDERBACK

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(7)(ii)(E)

ISO 27001:2013 6.1.3, 8.3, A.13.1.1, A.14

NIST SP 800-37 3.3, 3.4

NIST SP 800-53 AC-3, AC-17-18, AC-20, PL-2, PL-7-8, SC-7-8, SC-10

NIST Cybersecurity Framework ID.AM-6, ID.RM-1, PR.AC-5, PR.DS-1-2, DE.CM-1

PCI 2.1-3, 2.5-6, 4.1, 5.1

WORKSTATION SECURITY POLICY

Policy Area	IT Policy Library
Approved Date	June 30, 2020
Approved By	Policy Committee
Effective Date	July 1, 2020
Current Version	2.1

I. Overview

This document describes a required minimal security configuration for all workstations connected to a production network or used in a production capacity at or on behalf of F2Onsite.

II. Purpose

The purpose of this policy is to ensure the security of F2Onsite Information Systems, workstations, and data.

III. Scope

This policy applies to all Staff that use F2Onsite Information Systems.

IV. Policy

This Policy helps ensure that access to sensitive information is restricted to authorized users. By following appropriate security measures, Staff can help ensure information integrity, confidentiality, and availability.

Staff shall follow appropriate guidelines and procedures when using workstations and systems. F2Onsite has implemented certain technical, physical, and administrative controls and safeguards to ensure that workstations restrict access to authorized users

Physical access to workstations shall be restricted to only authorized personnel. Staff shall prevent unauthorized viewing of information on a screen:

- Staff shall ensure that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to prevent public viewing.
- Staff shall manually activate a password protected screen saver when they leave their desk.

- Systems shall have a password protected screen saver activated within a short timeout period to ensure that workstations that were left unsecured are protected.

Prior to leaving for the day, staff shall:

- Exit running applications and close any open documents.
- Ensure workstations are left on but logged off in order to facilitate after hours updates.

Staff shall comply with all applicable policies and procedures including:

- Acceptable Use Policy
- Anti-Malware Policy
- Mobile Device Policy
- Password Policy
- Remote Access Policy
- Wireless Access Policy

Staff shall use workstations for authorized business purposes only and only approved personnel may install pre-approved software on workstations.

All sensitive information must be stored on network servers. Sensitive information shall be encrypted and comply with F2Onsite's Encryption Policy. Laptops containing sensitive information shall have the hard drives encrypted and laptops shall be secured through the use of cable locks or locking laptops up in drawers or cabinets.

The IT Department shall ensure that all workstations use a surge protector (not just a power strip) or a UPS battery backup. Staff shall keep food and drink away from workstations in order to avoid accidental spills.

Workstations shall have vendor-issued critical security updates and patches installed in a timely manner. Refer to the Patch Management Policy for more information.

Workstations shall have active and updated anti-malware protection software. Staff shall not disable anti-malware protection software. See Anti-Malware Policy for more information.

Each workstation shall have an active software firewall that protects the device from external threats. Staff shall not disable the firewall.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all F2Onsite Staff that use Information Resources.

Policy History

Version	Date	Description	Approved By
2.1	07/01/2020	Initial policy release	D LAUDERBACK

References:

COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 32
HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
ISO 27001:2013 8.3, A.6.2, A.11.2, A.12.2, A.12.6
NIST SP 800-37 3.3, 3.7
NIST SP 800-53 AC-7(2), AC-11, AC-17, AC-18, AC-19, AT-2, MP-2, MP-4, SI-3, SI-4(24)
NIST Cybersecurity Framework ID.RA-6, PR.AC-2, PR.DS-3, PR.IP-5, DE.CM-1, RS.RP-1
PCI 1.4, 2.1, 6.2, 9.1

RECEIPT AND ACKNOWLEDGEMENT

I have read and been informed about the content, requirements, and expectations listed in ABC Company's (Company's) Policies and Plans. I understand that I am responsible for complying with the requirements stated in the Policies and Plans and I agree to abide by them as consideration for my continued employment by Company. I understand that:

- Violation of the Policies and Plans may result in disciplinary action including, but not limited to, termination.
- Company's Policies and Plans are located and maintained on Company's network and I have access to such network and Policies and Plans. I further understand that it is my responsibility to periodically check the network for updates to Company's Policies and Plans.
- Company's Policies, Plans, and descriptions of security controls are confidential and may not be distributed in any way nor discussed with anyone who is not a Staff member of Company.
- If any of the provisions of Company's Policies and Plans are found null, void, or inoperative for any reason, the remaining Policies and Plans will remain in full force and effect.

If I am uncertain about any Policy or Plan, I will check with my immediate supervisor or Company management.

Employee Signature

Date

Employee Name (Printed)