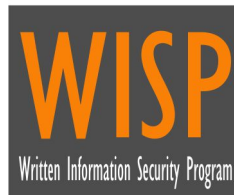


Your Logo
Will Be
Placed Here

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Business Consulting, LLC

ISO 27002



INTERNAL USE

Access Limited to Internal Use Only

***IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES
WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)***

Table of Contents

OVERVIEW, INSTRUCTIONS & EXAMPLE	11
Key Terminology	11
Overview	11
Customization Guidance	11
Validating Needs for Procedures / Control Activities	11
Procedures Documentation	11
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	12
Example Procedure	13
Supporting Policies & Standards	15
KNOWN COMPLIANCE REQUIREMENTS	16
Statutory Requirements	16
Regulatory Requirements	16
Contractual Requirements	16
INFORMATION SECURITY POLICY STRUCTURE	17
1.0 Information Security Program	17
1.1 Management Direction for Information Security	17
1.1.1 Policies for Information Security	17
1.1.1.1 Publishing An Information Security Policy	17
1.1.1.2 Information Security Program Plan	18
1.1.1.3 Assigned Information Security Responsibilities	18
1.1.1.4 Information Security Resources	19
1.1.1.5 Risk Management	20
1.1.2 Review of Information Security Policies	21
1.1.2.1 Information Security Documentation Review	21
ORGANIZATION OF INFORMATION SECURITY	22
2.0 Information Security Organization	22
2.1 Internal Organization	22
2.1.1 Information Security Roles and Responsibilities	22
2.1.1.1 Roles & Responsibilities	22
2.1.1.2 Position Categorization	23
2.1.2 Segregation of Duties	23
2.1.2.1 Incompatible Roles	23
2.1.2.2 Two-Person Rule	24
2.1.3 External Authorities	25
2.1.3.1 Contacts With Authorities	25
2.1.4 Special Interest Groups	26
2.1.4.1 Contacts With Security Groups & Associations	26
2.1.4.2 Security Industry Alerts & Notification Process	26
2.1.5 Information Security in Project Management	27
2.1.5.1 Security Assessments	27
2.1.5.2 System Security Plan (SSP)	28
2.2 Mobile Devices and Teleworking	29
2.2.1 Mobile Device Management	29
2.2.1.1 Access Control For Mobile Devices	30
2.2.1.2 Central Management Of Mobile Devices	31
2.2.1.3 Remote Purging	32
2.2.1.4 Personally Owned Devices	32
2.2.1.5 Tamper Protection & Detection	33
2.2.2 Teleworking	34
2.2.2.1 Telecommuting	34
2.2.2.2 Remote Access	35
2.2.2.3 Privileged Commands & Access	36
2.2.2.4 Non-Local Maintenance	36

2.2.2.5	Non-Local Maintenance Approvals & Notifications	37
2.2.2.6	Non-Local Maintenance Cryptographic Protection	38
2.2.2.7	Remote Disconnect Verification	38
2.2.2.8	Auditing	39
HUMAN RESOURCE SECURITY		40
3.0	Human Resource Security	40
3.1	Prior to Employment	40
3.1.1	Screening	40
3.1.1.1	Personnel Screening	40
3.1.2	Terms and Conditions of Employment	41
3.1.2.1	Access Agreements	41
3.2	During Employment	42
3.2.1	Management Responsibilities	42
3.2.1.1	Rules of Behavior	42
3.2.1.2	Social Media & Social Networking Restrictions	43
3.2.1.3	Position Categorization	43
3.2.1.4	Third-Party Personnel Security	44
3.2.2	Information Security Awareness, Education and Training	45
3.2.2.1	Information Security Workforce	45
3.2.2.2	Security Training	46
3.2.2.3	Awareness Training for Sensitive Information	46
3.2.2.4	Vendor Security Training	47
3.2.2.5	Security Training Records	48
3.2.2.6	Security Awareness	48
3.2.2.7	Testing, Training & Monitoring	49
3.2.2.8	Practical Exercises	50
3.2.2.9	Insider Threat Awareness	51
3.2.2.10	Security Industry Alerts & Notification Process	52
3.2.3	Disciplinary Process	53
3.2.3.1	Personnel Sanctions	53
3.2.3.2	Workplace Investigations	53
3.3	Termination and Change of Employment	54
3.3.1	Termination or Change of Employment Responsibilities	54
3.3.1.1	Personnel Termination	54
3.3.1.2	High-Risk Terminations	56
3.3.1.3	Personnel Transfer	56
ASSET MANAGEMENT		58
4.0	Asset Management	58
4.1	Responsibility for Assets	58
4.1.1	Inventory of Assets	58
4.1.1.1	Information System Inventory	58
4.1.1.2	Information System Component Inventory	59
4.1.1.3	Approved Deviations	59
4.1.1.4	Network Diagrams	60
4.1.2	Ownership of Assets	61
4.1.2.1	Default Settings	61
4.1.2.2	Shared Hosting Providers	61
4.1.2.3	Intranets	62
4.1.3	Acceptable Use of Assets	63
4.1.3.1	Rules of Behavior	63
4.1.3.2	Social Media & Social Networking Restrictions	64
4.1.3.3	Acceptable Use for Critical Technologies	64
4.1.4	Return of Assets	65
4.1.4.1	Asset Collection	65
4.2	Information Classification	66
4.2.1	Classification of Information	66
4.2.1.1	Security Categorization	66

4.2.2	Labeling of Information	67
4.2.2.1	Media Marking	67
4.2.3	Handling of Assets	67
4.2.3.1	Media Transportation	68
4.2.3.2	Media Custodians	68
4.2.3.3	Cryptographic Protection (Encrypting Data In Storage Media)	69
4.3	Media Handling	70
4.3.1	Management of Removable Media	70
4.3.1.1	Media Use	70
4.3.1.2	Media Access	70
4.3.2	Disposal of Media	71
4.3.2.1	Data Retention & Disposal	72
4.3.2.2	Media Sanitization	73
4.3.2.3	Media Sanitization Documentation	73
4.3.3	Physical Media Transfer	74
4.3.3.1	Strict Control of Media	74
ACCESS CONTROL		76
5.0	Access Control	76
5.1	Business Requirements of Access Control	76
5.1.1	Access Control	76
5.1.1.1	Identification & Authentication	76
5.1.1.2	Access To Sensitive Data	77
5.1.1.3	Access Control Procedures	77
5.1.2	Access to Networks and Network Services	78
5.1.2.1	Least Functionality	78
5.1.2.2	Prevent Program Execution	79
5.2	User Access Management	80
5.2.1	User Registration and De-Registration	80
5.2.1.1	User ID Management	80
5.2.1.2	Account Management	81
5.2.2	User Access Provisioning	82
5.2.2.1	Account Provisioning	82
5.2.2.2	Role-Based Access Control (RBAC)	83
5.2.3	Management of Privileged Access Rights	84
5.2.3.1	Privileged Commands & Access	84
5.2.4	Management of Secret Authentication Information of Users	84
5.2.4.1	User Identification & Authentication for Organizational Users	85
5.2.4.2	Multifactor Authentication	85
5.2.4.3	Identifier Management (User Names)	86
5.2.4.4	Privileged Account Management	88
5.2.4.5	Identification & Authentication (Non-Organizational Users)	89
5.2.4.6	Service Provider Identification & Authentication (Vendors)	90
5.2.5	Review of User Access Rights	90
5.2.5.1	Periodic Review	91
5.2.6	Removal or Adjustment of Access Rights	91
5.2.6.1	Access Enforcement	91
5.3	User Responsibilities	92
5.3.1	Use of Secret Authentication Information	92
5.3.1.1	Individual Credentials	92
5.3.1.2	Credential Sharing	93
5.4	System and Application Access Control	94
5.4.1	Information Access Restriction	94
5.4.1.1	Access Control Lists (ACLs)	94
5.4.1.2	Database Access	95
5.4.2	Secure Log-On Procedures	96
5.4.2.1	Trusted Communications Path	96
5.4.2.2	Device-To-Device Identification & Authentication	96
5.4.2.3	System Use Notification (Logon Banners)	97

5.4.2.3.1	System Use Notification Standardized Microsoft Windows Logon Banner	98
5.4.2.3.2	System Use Notification Truncated Logon Banner	99
5.4.2.4	Previous Logon Notification	99
5.4.3	Password Management System	100
5.4.3.1	Authenticator Management (Passwords)	100
5.4.3.2	Vendor-Supplied Defaults	101
5.4.3.3	Authenticator Feedback	102
5.4.3.4	Cryptographic Module Authentication	103
5.4.3.5	Re-Authentication	103
5.4.4	Use of Privileged Utility Programs	104
5.4.4.1	Access Enforcement	104
5.4.4.2	Least Privilege	105
5.4.5	Access Control to Program Source Code	106
5.4.5.1	Source Code	106
5.4.5.2	Library Privileges	106
ENCRYPTION		108
6.0	Cryptography	108
6.1	Cryptographic Controls	108
6.1.1	Use of Cryptographic Controls	108
6.1.1.1	Use of Cryptography	108
6.1.1.2	Transmission Confidentiality	109
6.1.1.3	Non-Local Maintenance Cryptographic Protection	110
6.1.1.4	Wireless Access Authentication & Encryption	110
6.1.1.5	Encrypting Data At Rest	111
6.1.1.6	Non-Console Administrative Access	112
6.1.2	Key management	112
6.1.2.1	Key Management Program	112
6.1.2.2	Key Management Processes	113
PHYSICAL & ENVIRONMENTAL SECURITY		115
7.0	Physical and Environmental Security	115
7.1	Secure Areas	115
7.1.1	Physical Security Perimeter	115
7.1.1.1	Physical Access Authorizations	115
7.1.1.2	Role-Based Physical Access	116
7.1.1.3	Identification Requirement	116
7.1.1.4	Restrict Unescorted Access	117
7.1.1.5	Physical Access Control	118
7.1.1.6	Physical Access Logs	119
7.1.1.7	Lockable Physical Casings	119
7.1.1.8	Access Control For Transmission Medium	120
7.1.1.9	Access Control For Output Devices	121
7.1.1.10	Monitoring Physical Access	122
7.1.1.11	Visitor Control	122
7.1.1.12	Access Records	123
7.1.2	Physical Entry Controls	124
7.1.2.1	Facility Entry Controls	124
7.1.2.2	Authorizing & Monitoring Visitors	125
7.1.2.3	Distinguish Visitors from On-Site Personnel	126
7.1.3	Securing Offices, Rooms and Facilities	126
7.1.3.1	Physical Access Controls to Sensitive Areas	126
7.1.3.2	Physically Secure All Media	127
7.1.4	Protecting Against External and Environmental Threats	128
7.1.4.1	Risk Assessment	128
7.1.4.2	Risk Ranking	129
7.1.4.3	Security Industry Alerts & Notification Process	130
7.1.4.4	Threat Analysis & Flaw Remediation	131
7.1.5	Working in Secure Areas	131

7.1.5.1	Workstation Security	131
7.1.6	Delivery and Loading Areas	132
7.1.6.1	Delivery & Removal	132
7.2	Equipment	133
7.2.1	Equipment Siting and Protection	133
7.2.1.1	Location of Information System Components	133
7.2.1.2	Media Storage	134
7.2.2	Supporting Utilities	135
7.2.2.1	Automatic Voltage Controls	135
7.2.2.2	Emergency Shutoff	135
7.2.2.3	Emergency Power	136
7.2.2.4	Emergency Lighting	137
7.2.2.5	Fire Protection	137
7.2.2.6	Fire Detection Devices	138
7.2.2.7	Fire Suppression Devices	139
7.2.2.8	Temperature & Humidity Controls	139
7.2.2.9	Water Damage Protection	140
7.2.3	Cabling Security	141
7.2.3.1	Power Equipment & Power Cabling	141
7.2.4	Equipment Maintenance	141
7.2.4.1	Controlled Maintenance	141
7.2.4.2	Maintenance Activities	143
7.2.4.3	Maintenance Tools	143
7.2.4.4	Maintenance Personnel	144
7.2.4.5	Timely Maintenance	144
7.2.5	Removal of Assets	145
7.2.5.1	Delivery & Removal	145
7.2.6	Security of Equipment and Assets Off-Premises	146
7.2.6.1	Media Distribution	146
7.2.7	Secure Disposal or Re-Use of Equipment	147
7.2.7.1	Media Destruction	147
7.2.8	Unattended User Equipment	148
7.2.8.1	Device Storage in Automobiles	148
7.2.8.2	Kiosks & Point of Sale Devices	148
7.2.9	Clear Desks and Clear Screens	149
7.2.9.1	Workplace Security	149
OPERATIONS SECURITY		151
8.0	Operations Security	151
8.1	Operational Procedures and Responsibilities	151
8.1.1	Documented Operating Procedures	151
8.1.1.1	Security Concept of Operations (CONOPS)	151
8.1.1.2	Operational Security (OPSEC)	151
8.1.1.3	System Security Plans	152
8.1.2	Change Management	153
8.1.2.1	Configuration Change Control	153
8.1.2.2	Prohibition of Changes	154
8.1.2.3	Security Representative for Changes	155
8.1.2.4	Security Impact Analysis for Changes	156
8.1.2.5	Configuration Management	156
8.1.2.6	Baseline Configurations	157
8.1.2.7	Baseline Configuration Reviews & Updates	159
8.1.2.8	Retention of Previous Configurations	160
8.1.2.9	Network Device Configuration File Synchronization	160
8.1.3	Capacity Management	161
8.1.3.1	Capacity Management	161
8.1.4	Separation of Development, Testing and Operational Environments	162
8.1.4.1	Separate Development & Test Environments	162
8.2	Protection from Malware	162

8.2.1	Controls Against Malware	163
8.2.1.1	Antimalware Mechanisms	163
8.2.1.2	Antimalware Installation	163
8.2.1.3	Antimalware Signature Updates	164
8.2.1.4	Malware Protection Procedures	165
8.3	Backup	165
8.3.1	Information Backup	165
8.3.1.1	Information System Backup	166
8.3.1.2	Information System Recovery & Reconstitution	166
8.3.1.3	Transaction Recovery	167
8.3.1.4	Failover Capability	168
8.3.1.5	Electronic Discovery (eDiscovery)	168
8.3.1.6	Information System Imaging	169
8.3.1.7	Backup & Restoration Hardware Protection	170
8.4	Logging and Monitoring	170
8.4.1	Event Logging	170
8.4.1.1	Automated Audit Trails	170
8.4.1.2	Audit Trail Content	172
8.4.1.3	Log Review	172
8.4.1.4	Linking Access to Individual Users	173
8.4.1.5	File Integrity Monitoring (FIM)	174
8.4.2	Protection of Log Information	175
8.4.2.1	Securing Audit Trails	175
8.4.2.2	Retention of Audit Trail History	175
8.4.3	Administrator and Operator Logs	176
8.4.3.1	Privileged Functions Logging	176
8.4.4	Clock Synchronization	177
8.4.4.1	Network Time Protocol (NTP)	177
8.5	Control of Operational Software	178
8.5.1	Installation of Software on Operational Systems	178
8.5.1.1	Access Restriction for Change	178
8.6	Technical Vulnerability Management	178
8.6.1	Management of Technical Vulnerabilities	178
8.6.1.1	Software Patching	179
8.6.1.2	Vulnerability Scanning	180
8.6.1.3	Penetration Testing	180
8.6.1.4	Vulnerability Ranking	181
8.6.1.5	Vulnerability Remediation	182
8.6.2	Restrictions on Software Installation	183
8.6.2.1	User-Installed Software	183
8.6.2.2	Unauthorized Installation Alerts	184
8.6.2.3	Prohibit Installation Without Privileged Status	184
8.7	Information Systems Audit Considerations	185
8.7.1	Information Systems Audit Controls	185
8.7.1.1	Security-Related Activity Planning	185
COMMUNICATIONS SECURITY		187
9.0	Communications Security	187
9.1	Network Security Management	187
9.1.1	Network Controls	187
9.1.1.1	Firewall & Router Configurations	187
9.1.1.2	Safeguarding Data Over Open Networks	188
9.1.1.3	Transmitting Sensitive Data	189
9.1.1.4	Rogue Wireless Detection	189
9.1.1.5	Intrusion Detection & Prevention Systems	190
9.1.2	Security of Network Services	191
9.1.2.1	Restricting Connections	191
9.1.3	Segregation in Networks	192
9.1.3.1	Security Function Isolation	192

9.1.3.2	Layered Defenses	193
9.1.3.3	Application Partitioning	194
9.2	Information Transfer	195
9.2.1	Information Transfer Policies and Procedures	195
9.2.1.1	Direct Internet Access	195
9.2.2	Agreements on Information Transfer	196
9.2.2.1	Access Agreements for Information Transfer	196
9.2.3	Electronic Messaging	197
9.2.3.1	Transmission Confidentiality	197
9.2.3.2	Ad-Hoc Transfers	198
9.2.3.3	Communications Technologies	198
9.2.3.4	Intranets	199
9.2.4	Confidentiality or Non-Disclosure Agreements (NDAs)	200
9.2.4.1	Business Partner Contracts	200
9.2.4.2	Third-Party Personnel Security	201
9.2.4.3	Monitoring for Information Disclosure	202
SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE		203
10.0	System Acquisition, Development and Maintenance	203
10.1	Security Requirements of Information Systems	203
10.1.1	Information Security Requirements Analysis and Specification	203
10.1.1.1	Secure Configurations	203
10.1.2	Securing Application Services on Public Networks	205
10.1.2.1	Software Firewall	205
10.1.3	Protecting Application Services Transactions	206
10.1.3.1	Transmission Integrity	206
10.2	Security in Development and Support Processes	206
10.2.1	Secure Development	206
10.2.1.1	Application Development	206
10.2.2	System Change Control Procedures	207
10.2.2.1	Change Control	207
10.2.2.2	Secure Coding Principles	208
10.2.3	Technical Review of Applications After Operating Platform Changes	209
10.2.3.1	Test, Validate & Document Changes	209
10.2.3.2	Security Functionality Verification	210
10.2.4	Restrictions on Changes to Software Packages	210
10.2.4.1	Library Privileges	210
10.2.5	Secure System Engineering Principles	211
10.2.5.1	Secure System Engineering Principles	211
10.2.5.2	Ports, Protocols & Services Documentation	212
10.2.6	Secure Development Environment	213
10.2.6.1	Development Environments	213
10.2.7	Outsourced Development	213
10.2.7.1	External Service Providers	213
10.2.7.2	Developer Configuration Management	214
10.2.8	System Security Testing	215
10.2.8.1	Security Assessments	215
10.2.8.2	Plan of Action & Milestones (POA&M)	216
10.2.9	System Acceptance Testing	217
10.2.9.1	Security Authorization	217
10.3	Test Data	218
10.3.1	Protection of Test Data	218
10.3.1.1	Use of Live Data	218
10.3.1.2	Test Data Integrity	219
10.3.1.3	Information Output Handling & Retention	219
VENDOR MANAGEMENT		221
11.0	Supplier Relationships	221
11.1	Information Security in Supplier Relationships	221

11.1.1	Information Security Policy for Supplier Relationships	221
11.1.1.1	Service Provider Management	221
11.1.1.2	System Development Life Cycle (SDLC)	222
11.1.1.3	Acquisition Process	222
11.1.1.4	Commercial Off-The-Shelf (COTS) Security Solutions	223
11.1.1.5	Functional Properties of Security Controls	224
11.1.1.6	Design & Implementation of Security Controls	225
11.1.1.7	Development Methods	225
11.1.1.8	Developer Documentation	227
11.1.2	Addressing Security Within Supplier Agreements	232
11.1.2.1	Service Provider Accountability	232
11.1.2.2	Validate as Genuine & Not Altered	233
11.1.2.3	Limitation From Harm	234
11.1.3	Information and Communication Technology Supply Chain	235
11.1.3.1	Supply Chain Protection	235
11.1.3.2	Acquisition Strategies, Tools & Methods	235
11.1.3.3	Criticality Analysis	236
11.1.3.4	Trustworthiness	237
11.2	Supplier Service Delivery Management	238
11.2.1	Monitoring and Review of Supplier Services	238
11.2.1.1	Supplier Reviews	238
11.2.1.2	Supplier Weakness or Deficiency Remediation	239
11.2.1.3	Development Process, Standards & Tools	239
11.2.2	Managing Changes to Supplier Services	241
11.2.2.1	Developer Configuration Management	241
11.2.2.2	Developer Security Testing	242
11.2.2.3	Developer Code Analysis	243
11.2.2.4	Developer Threat Analysis & Flaw Remediation	243
INCIDENT RESPONSE		245
12.0	Information Security Incident Management	245
12.1	Management of Information Security Incidents and Improvements	245
12.1.1	Responsibilities and Procedures	245
12.1.1.1	Incident Response	245
12.1.1.2	Incident Response Training	246
12.1.2	Reporting Information Security Events	246
12.1.2.1	Incident Reporting	246
12.1.3	Reporting Information Security Weaknesses	247
12.1.3.1	Reporting Weaknesses	247
12.1.3.2	Incident Reporting Assistance	248
12.1.4	Assessment of and Decision on Information Security Events	249
12.1.4.1	Integrated Security Incident Response Team	249
12.1.5	Response to Information Security Incidents	249
12.1.5.1	Incident Response Plan (IRP)	249
12.1.6	Learning from Information Security Incidents	251
12.1.6.1	Incident Response Lessons Learned	251
12.1.7	Collection of Evidence	251
12.1.7.1	Incident Handling	251
12.1.7.2	Information Spillage Response	252
BUSINESS CONTINUITY MANAGEMENT		254
13.0	Business Continuity Management	254
13.1	Information Security Continuity	254
13.1.1	Planning Information Security Continuity	254
13.1.1.1	Contingency Plan	254
13.1.1.2	Contingency Training	255
13.1.2	Implementing Information Security Continuity	255
13.1.2.1	Contingency Planning Procedures	256
13.1.3	Verify, Review and Evaluate Information Security Continuity	256

13.1.3.1	Contingency Testing & Exercises	257
13.1.3.2	Contingency Plan Update	257
13.2	Redundancies	258
13.2.1	Availability of Information Processing Facilities	258
13.2.1.1	Alternate Storage Site	258
13.2.1.2	Alternate Processing Site	259
13.2.1.3	Telecommunications Services	260
13.2.1.4	Priority of Service Provisions Storage Site	260
INFORMATION SECURITY COMPLIANCE		262
14.0	Compliance	262
14.1	Compliance with Legal and Contractual Requirements	262
14.1.1	Identification of Applicable Legislation and Contractual Requirements	262
14.1.1.1	Regulatory & Non-Regulatory Compliance	262
14.1.2	Intellectual Property Rights	263
14.1.2.1	Software Usage Restrictions	263
14.1.3	Protection of Records	264
14.1.3.1	Minimizing Sensitive Data Storage	264
14.1.3.2	Data Masking	264
14.1.3.3	Storing Authentication Data	265
14.1.3.4	Making Sensitive Data Unreadable In Storage	266
14.1.4	Privacy and Protection of Personal Data	267
14.1.4.1	Minimization Of Personal Data (PD)	267
14.1.4.2	Data Retention & Disposal	268
14.1.4.3	Data Collection	269
14.1.4.4	Sensitive Data Storage	269
14.1.5	Regulation of Cryptographic Controls	270
14.1.5.1	Export-Controlled Information	270
14.2	Information Security Reviews	271
14.2.1	Independent Review of Information Security	271
14.2.1.1	Independent Assessors	271
14.2.2	Compliance with Security Policies and Standards	272
14.2.2.1	Security Assessments	272
14.2.3	Technical Compliance Review	273
14.2.3.1	Functional Properties Of Security Controls	273
GLOSSARY: ACRONYMS & DEFINITIONS		274
Acronyms		274
Definitions		274
RECORD OF CHANGES		275

OVERVIEW, INSTRUCTIONS & EXAMPLE

KEY TERMINOLOGY

With the Cybersecurity Standardized Operating Procedures (CSOP), it is important to understand a few key terms:

- **Procedure / Control Activity:** Procedures represent an established way of doing something, such as a series of actions conducted in a specified order or manner. Some organizations refer to procedures as “control activities” and the terms essentially synonymous. In the CSOP, the terms procedure or control activity can be used interchangeably.
- **Process Owner:** This is the name of the individual or team accountable for the procedure being performed. This identifies the *accountable party to ensure the procedure is performed*. This role is more oversight and managerial.
 - Example: The **Security Operations Center (SOC) Supervisor** is accountable for his/her team to collect log files, perform analysis and escalate potential incidents for further investigation.
- **Process Operator:** This is the name of the individual or team responsible to perform the procedure’s tasks. This identifies the *responsible party for actually performing the task*. This role is a “doer” and performs tasks.
 - Example: The **SOC analyst** is responsible for performing daily log reviews, evaluating anomalous activities and responding to potential incidents in accordance with the organization’s Incident Response Plan (IRP).

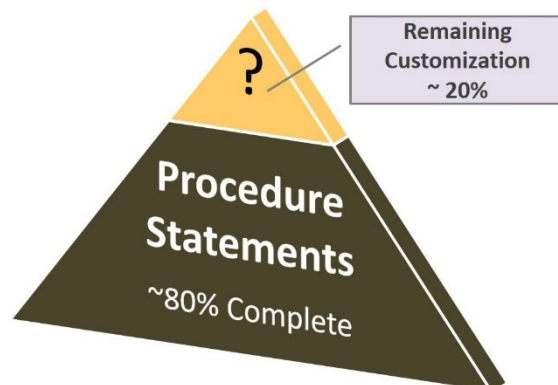
OVERVIEW

The Cybersecurity Standardized Operating Procedures (CSOP) is a catalog of procedure/control activity statements. These are templates that require slight modification to suit the specific needs of the organization,

CUSTOMIZATION GUIDANCE

The content of the CSOP does require a certain level of customization by any organization, since every organization has some difference in available people, processes or technology that can be leveraged to perform these procedures/control activities.

Essentially, we’ve done the heavy lifting in developing the template and pre-populating a significant amount of content. Our target is about 80% of the content as part of the template that would leave the remaining 20% for customization with specifics that only the organization would know, such as the organization calls the change management group the Change Advisory Board (CAB) instead of the Change Control Board (CCB). Those little changes in roles, titles, department naming, technologies in use are all content that just needs to be filled into the template to finalize the procedures/control activities.



VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES

Procedures are not meant to be documented for the sake of generating paperwork - procedures are meant to satisfy a specific operational need that are complied with:

- If procedures exist and are not tied to a standard, then management should review why the procedure is in place.
- A procedure that lacks a mapping to a standard may indicate “mission creep” and represent an opportunity to reassign the work or cease performing the procedure.

PROCEDURES DOCUMENTATION

The objective of the CSOP is to provide management direction and support for cybersecurity in accordance with business requirements, as well as relevant laws, regulations and contractual obligations.

Procedures should be both clearly-written and concise.

- Procedure documentation is meant to provide evidence of due diligence that standards are complied with.
- Well-managed procedures are critical to a security program, since procedures represents the specific activities that are performed to protect systems and data.

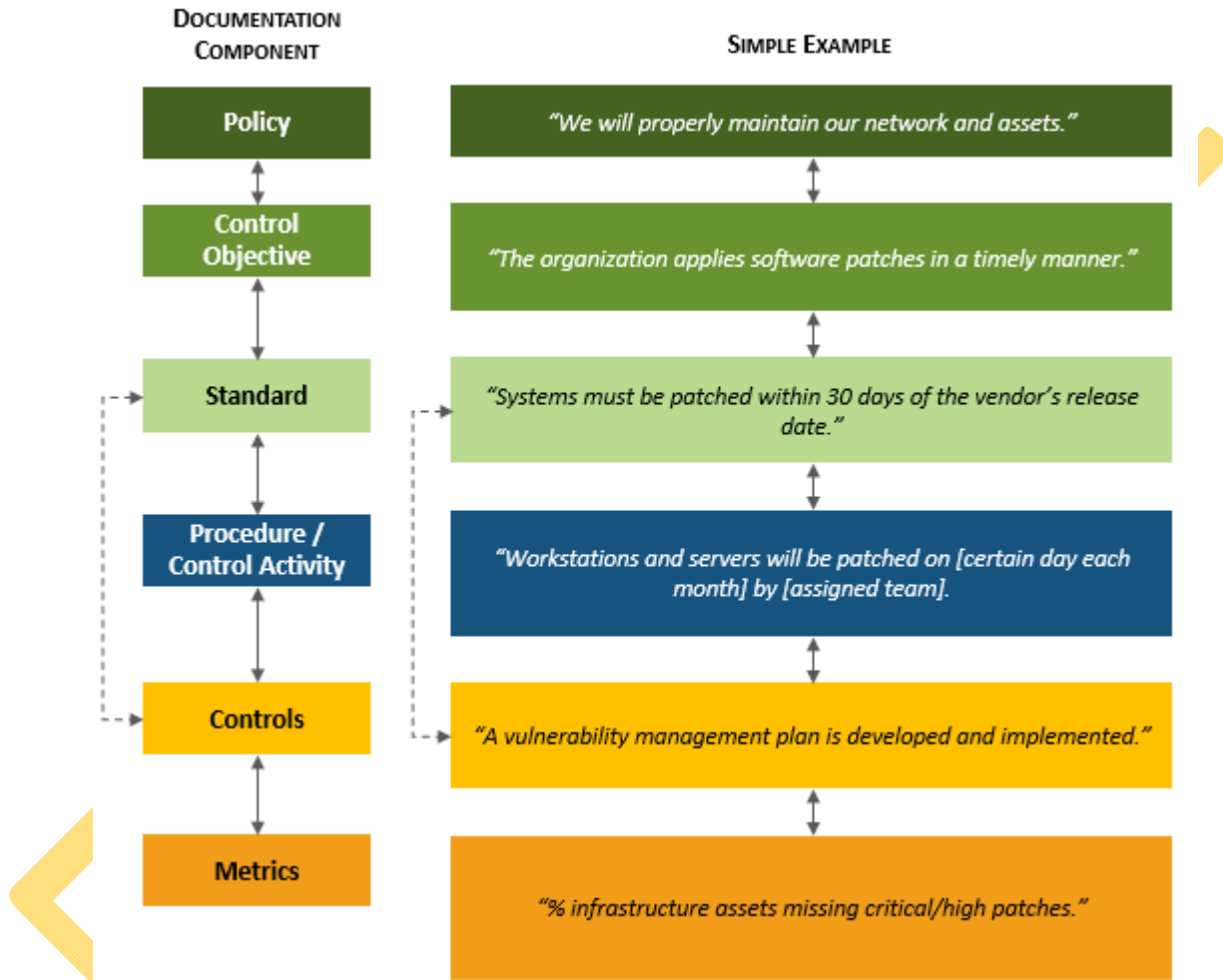
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

From a due care and due diligence perspective, it can be thought of this way:

- Certain standards require processes to exist (*due care – evidence demonstrates standards exist*).
- Performing the activities outlined in a procedure and documenting the work that was performed satisfies the intent of the standard (*due diligence – evidence demonstrates the standard is operating effectively*).

The diagram shown below helps visualize the linkages in documentation that involve written procedures:

- CONTROL OBJECTIVES exist to support POLICIES;
- STANDARDS are written to support CONTROL OBJECTIVES;
- PROCEDURES are written to implement the requirements that STANDARDS establish;
- CONTROLS exist as a mechanism to assess/audit both the existence of PROCEDURES / STANDARDS and how well their capabilities are implemented and/or functioning; and
- METRICS exist as a way to measure the performance of CONTROLS.



Documentation Flow Example.

NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK

The CSOP leverages the NIST NICE Cybersecurity Workforce Framework.¹ The purpose of this framework is that work roles have an impact on an organization's ability to protect its data, systems and operations. By assigning work roles, it helps direct the work of employees and contractors to minimize assumptions about who is responsible for certain cybersecurity and privacy tasks.

The CSOP uses the work roles identified in the NIST NICE Cybersecurity Workforce Framework to help make assigning the tasks associated with procedures/control activities more efficient and manageable. Keep in mind these are merely recommendations and are fully editable for every organization – this is just a helpful point in the right direction!

¹ NIST NICE Cybersecurity Workforce Framework - <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>



NIST NICE Cybersecurity Workforce Framework – Work Categories

EXAMPLE PROCEDURE

This example is a configuration procedure from section **10.1.1.1 (Secure Configurations)**

PLEASE NOTE THE PROCESS CRITERIA SECTION SHOWN BELOW CAN BE DELETED & IS NOT PART OF THE PROCEDURE

The process criteria sections exist only to be a useful tool to help build out the procedures by establishing criteria and creating a working space to capture key components that impacts the procedure.

Process Criteria:

- Process Owner: name of the individual or team accountable for the procedure being performed
 - *Example: The process owner for system hardening at ACME is the cybersecurity director, John Doe.*
- Process Operator: name of the individual or team responsible to perform the procedure’s tasks.
 - *Example: The process operator for system hardening at ACME is split between several teams:*
 - *Network gear is assigned to network admins.*
 - *Servers are assigned to server admins.*
 - *Laptops, desktops and mobile devices are assign to the End User Computing (EUC) team.*
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
 - *Example: Generally, system hardening is an “as needed” process that happens when new operating systems are released or when new technology is purchased. However, there should still be an annual review to ensure that appropriate baseline configurations exist and are current to what is deployed at ACME.*
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
 - *Example: The scope affects the entire company. Any deviations to the secure baselines are handled on an individual basis.*
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
 - *Example: Baseline configurations, benchmarks and STIGs are located on server XYZ123 in the folder called “Secure Baselines” and it is available for read-only for all users.*
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
 - *Example: There are no SLAs associated with baseline configurations.*
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?
 - *Example: The following classes of systems and applications are in scope for this procedure:*
 - *Server-Class Systems*
 - *Workstation-Class Systems*
 - *Network Devices*
 - *Databases*

Control Objective: The organization develops and controls configuration standards for all system components that are consistent with industry-accepted system hardening standards.² *[the control objective is meant to address the statutory, regulatory and contractual requirements identified in the footnote (see bottom of page in the footer section)]*

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with the Technical Support Specialist [OM-STS-001] and Security Architect [SP-ARC-002]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory, and regulatory compliance obligations.

² NIST 800-53 rev4 CM-2 & CM-6 | FedRAMP | NIST 800-171 3.4.1 & 3.4.2 | PCI DSS 1.1 & 1.1.1 | NIST CSF PR.IP-1 | DFARS 252.204-7008 | CSC 3.1 | CCM GRM-01 & IVS-07 | COBIT5 BAI10.02 | NISPOM 8-202, 8-311 & 8-610

- (2) Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to:
- a. Center for Internet Security (CIS) benchmarks;
 - b. Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs); or
 - c. Original Equipment Manufacturer (OEM) security configuration guides.
- (3) Ensures that system hardening includes, but is not limited to:
- a. Technology platforms that include, but are not limited to:
 - i. Server-Class Systems
 1. Microsoft Server 2003
 2. Microsoft Server 2008
 3. Microsoft Server 2012
 4. Microsoft Server 2016
 5. Red Hat Enterprise Linux (RHEL)
 6. Unix
 7. Solaris
 - ii. Workstation-Class Systems
 1. Microsoft XP
 2. Microsoft 7
 3. Microsoft 8
 4. Microsoft 10
 5. Apple
 6. Fedora (Linux)
 7. Ubuntu (Linux)
 8. SuSe (Linux)
 - iii. Network Devices
 1. Firewalls
 2. Routers
 3. Load balancers
 4. Virtual Private Network (VPN) concentrators
 5. Wireless Access Points (WAPs)
 6. Wireless controllers
 7. Printers
 8. Multi-Function Devices (MFDs)
 - iv. Mobile Devices
 1. Tablets
 2. Mobile phones
 3. Other portable electronic devices
 - v. Databases
 1. MySQL
 2. Windows SQL Server
 3. Windows SQL Express
 4. Oracle
 5. DB2
 - b. Enforcing least functionality, which includes but is not limited to:
 - i. Allowing only necessary and secure services, protocols, and daemons;
 - ii. Removing all unnecessary functionality, which includes but is not limited to:
 1. Scripts;
 2. Drivers;
 3. Features;
 4. Subsystems;
 5. File systems; and
 6. Unnecessary web servers.
 - c. Configuring and documenting only the necessary ports, protocols, and services to meet business needs;
 - d. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS), or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP;
 - e. Installing and configuring appropriate technical controls, such as:

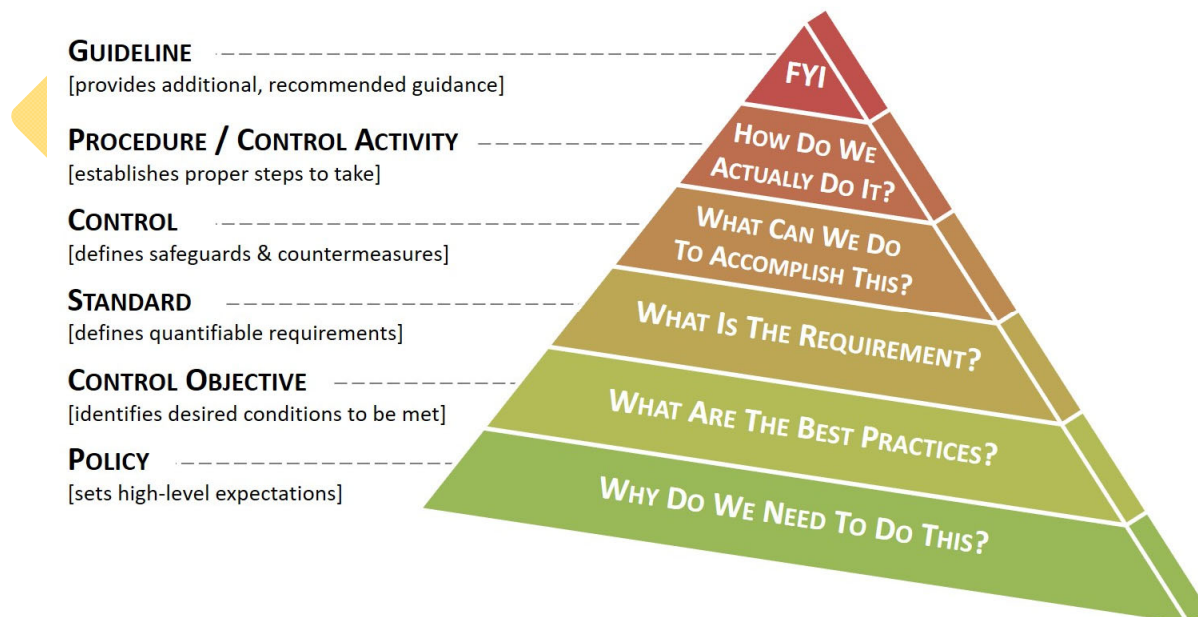
- i. Antimalware;
 - ii. Software firewall;
 - iii. Event logging; and
 - iv. File Integrity Monitoring (FIM), as required; and
 - f. As applicable, implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers).
- (4) Documents and validates security parameters are configured to prevent misuse.
 - (5) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning, or use.
 - (6) Validates and refreshes configurations on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. Unless a technical or business reason exists, standardized images are used to represent hardened versions of the underlying operating system and the applications installed on the system.
 - (7) On at least an annual basis, during the 2nd quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
 - a. Distributes copies of the change to key personnel; and
 - b. Communicates the changes and updates to key personnel.
 - (8) If necessary, requests corrective action to address identified deficiencies.
 - (9) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
 - (10) If necessary, documents the results of corrective action and notes findings.
 - (11) If necessary, requests additional corrective action to address unremediated deficiencies.

SUPPORTING POLICIES & STANDARDS

While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge's [ISO 27002-based Written Information Security Program \(WISP\)](#) that contains policies, control objectives, standards and guidelines.

Cybersecurity documentation is comprised of six (6) main parts:

- (1) Core policy that establishes management's intent;
- (2) Control objective that identifies leading practices;
- (3) Standards that provides quantifiable requirements;
- (4) Controls identify desired conditions that are expected to be met;
- (5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
- (6) Guidelines are recommended, but not mandatory.



Cybersecurity Documentation Hierarchy

2.1.4 SPECIAL INTEREST GROUPS

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.²¹

2.1.4.1 CONTACTS WITH SECURITY GROUPS & ASSOCIATIONS

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization establishes and institutionalizes contact with selected groups and associations within the security community to:²²

- Facilitate ongoing security education and training for organizational personnel;
- Maintain currency with recommended security practices, techniques and technologies; and
- Share current security-related information including threats, vulnerabilities and incidents.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Security Architect [SP-ARC-002] and Executive Cyber Leadership [OV-EXL-001]:

- (1) Researches, establishes and maintains formal contact with select groups and / or associations within the cybersecurity and communities. Security groups and associations include, but are not limited to:
 - a. Special Interest Groups (SIGs);
 - b. Professional associations; and
 - c. Peer groups of cybersecurity and privacy professionals in similar organizations.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
 - a. Distributes copies of the change to key personnel; and
 - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

2.1.4.2 SECURITY INDUSTRY ALERTS & NOTIFICATION PROCESS

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?

²¹ ISO/IEC 27002:2013 – 6.1.4

²² HIPAA 164.308(A)(5)(ii) & (ii)(A) | PCI DSS v3.2 5.1.2 & 6.1 | NIST CSF v1.1 ID.RA-2 & RS.CO-5 | NY DFS 500.10

2.2.1.1 ACCESS CONTROL FOR MOBILE DEVICES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization:²⁹

- Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;
- Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;
- Monitors for unauthorized connections of mobile devices to organizational information systems;
- Enforces requirements for the connection of mobile devices to organizational information systems;
- Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk; and
- Applies inspection measures to mobile devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.

Procedure / Control Activity: Systems Security Developer [SP-SYS-001], in conjunction with Identity & Access Specialist [XX-IAC-001] and Systems Security Manager [OV-MGT-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices to implement access control for mobile devices, in accordance with ACME policies and standards:
 - a. **Loss / Theft:** Immediately notify ACME management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device;
 - b. **Conduct:** Users must conduct themselves in accordance with ACME's Acceptable Use parameters (*Annex5: Rules of Behavior (Acceptable & Unacceptable Use)*);
 - c. **Passwords:** A password or PIN with a minimum of four (4) characters must be used to log onto the device
 - d. **Lockout:** The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.
 - e. **Encryption:** The data on the mobile device must be encrypted.
 - f. **Message Storage Limits:** Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
 - g. **Data Backups:** If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer) then the backup data must be encrypted.
 - h. **Software Protections:** Applications that create, store, access, send or receive ePHI must meet ACME security standards and custom developed applications used on mobile devices must undergo a security design review.
 - i. **Antimalware:** Antimalware software must be installed on mobile devices that are capable of running such software:
 - i. **Android:** Android devices are required to have antimalware software installed.
 - ii. **Windows:** Windows devices are required to have antimalware software installed.
 - iii. **Apple:** The Apple iOS is not currently capable of running antimalware software, since no such software exists, based on the design of the iOS.
 - j. **Updates:** Mobile device and installed applications must be kept updated with the latest vendor software releases:
 - i. **Operating Systems:** The most recent operating system available for the mobile data device must be used.

²⁹ ISO/IEC 27002:2013 – 6.2.1 | NIST CSF v1.1 PR.AC-3

- ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by ACME IT staff.
 - k. Rooting: Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., “jailbreaking”) and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.
 - l. Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
 - i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
 - ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
 - iii. Cellular: ACME is not responsible for overages or data plans for cellular usage.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
- a. Distributes copies of the change to key personnel; and
 - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

2.2.1.2 CENTRAL MANAGEMENT OF MOBILE DEVICES

Process Criteria: (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- Process Owner: name of the individual or team accountable for the procedure being performed
- Process Operator: name of the individual or team responsible to perform the procedure’s tasks
- Occurrence: how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- Scope of Impact: what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- Location of Additional Documentation: if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- Performance Target: if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- Technology in Use: if applicable, what is the name of the application/system/service used to perform the procedure?

Control Objective: The organization centrally manages mobile devices.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Security Architect [SP-ARC-002] and Executive Cyber Leadership [OV-EXL-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices to ensure are sufficient for managing mobile devices by:
- a. Centrally-managing a mobile device management solution;
 - b. Managing passwords in accordance with ACME’s existing password standards;
 - c. Maintaining an inventory of all authorized mobile devices used to store and access ACME data;
 - d. Defining approved application stores for mobile devices accessing or storing sensitive data; and
 - e. Alerting security personnel when mobile devices are rooted or jailbroken.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
- a. Distributes copies of the change to key personnel; and
 - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.