

YOUR LOGO GOES HERE

STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Professional Services, LLC



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	9
KEY TERMINOLOGY	9
OVERVIEW	9
CUSTOMIZATION GUIDANCE	9
VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES	9
PROCEDURES DOCUMENTATION	10
NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK	11
EXAMPLE	11
KNOWN COMPLIANCE REQUIREMENTS	14
STATUTORY REQUIREMENTS	14
REGULATORY REQUIREMENTS	14
CONTRACTUAL REQUIREMENTS	14
CYBERSECURITY & PRIVACY GOVERNANCE (GOV) PROCEDURES	15
P-GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM	15
P-GOV-01.1: DIGITAL SECURITY GOVERNANCE PROGRAM STEERING COMMITTEE	15
P-GOV-01.2: DIGITAL SECURITY GOVERNANCE PROGRAM STATUS REPORTING TO GOVERNING BODY	16
P-GOV-02: PUBLISHING SECURITY & PRIVACY DOCUMENTATION	17
P-GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY PROGRAM	17
P-GOV-04: ASSIGNED CYBERSECURITY & PRIVACY RESPONSIBILITIES	18
P-GOV-05: MEASURES OF PERFORMANCE	18
P-GOV-06: CONTACTS WITH AUTHORITIES	19
P-GOV-07: CONTACTS WITH GROUPS & ASSOCIATIONS	19
P-GOV-08: DEFINED BUSINESS CONTEXT & MISSION	19
P-GOV-09: DEFINED CONTROL OBJECTIVES	20
ASSET MANAGEMENT (AST) PROCEDURES	21
P-AST-01: ASSET GOVERNANCE	21
P-AST-01.1: ASSET GOVERNANCE ASSET-SERVICE DEPENDENCIES	21
P-AST-01.2: ASSET GOVERNANCE STAKEHOLDER IDENTIFICATION & INVOLVEMENT	21
P-AST-02: ASSET INVENTORIES	22
P-AST-02.7: ASSET INVENTORIES SOFTWARE LICENSING RESTRICTIONS	22
P-AST-02.8: ASSET INVENTORIES DATA ACTION MAPPING	23
P-AST-03: ASSET OWNERSHIP ASSIGNMENT	23
P-AST-03.1: ASSET OWNERSHIP ASSIGNMENT ACCOUNTABILITY INFORMATION	24
P-AST-03.2: ASSET OWNERSHIP ASSIGNMENT PROVENANCE	24
P-AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	25
P-AST-04.1: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) ASSET SCOPE CLASSIFICATION	25
P-AST-05: SECURITY OF ASSETS & MEDIA	26
P-AST-06: UNATTENDED END-USER EQUIPMENT	27
P-AST-07: KIOSKS & POINT OF INTERACTION (POI) DEVICES	27
P-AST-08: TAMPER DETECTION	27
P-AST-09: SECURE DISPOSAL, DESTRUCTION OR RE-USE OF EQUIPMENT	28
P-AST-10: RETURN OF ASSETS	28
P-AST-11: REMOVAL OF ASSETS	29
P-AST-12: USE OF PERSONAL DEVICES	29
P-AST-15: TAMPER PROTECTION	30
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) PROCEDURES	31
P-BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	31
P-BCD-01.1: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH RELATED PLANS	31
P-BCD-01.2: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH EXTERNAL SERVICE PROVIDERS	32
P-BCD-04: CONTINGENCY PLAN TESTING & EXERCISES	32
P-BCD-08: ALTERNATE STORAGE SITE	32
P-BCD-09: ALTERNATE PROCESSING SITE	33
P-BCD-11: DATA BACKUPS	33
P-BCD-11.1: DATA BACKUPS TESTING FOR RELIABILITY & INTEGRITY	34

P-BCD-11.2: DATA BACKUPS SEPARATE STORAGE FOR CRITICAL INFORMATION	35
P-BCD-11.4: DATA BACKUPS CRYPTOGRAPHIC PROTECTION	35
P-BCD-11.7: DATA BACKUPS REDUNDANT SECONDARY SYSTEM	35
CAPACITY & PERFORMANCE PLANNING (CAP) PROCEDURES	37
P-CAP-01: CAPACITY & PERFORMANCE MANAGEMENT	37
P-CAP-03: CAPACITY PLANNING	37
CHANGE MANAGEMENT (CHG) PROCEDURES	38
P-CHG-01: CHANGE MANAGEMENT PROGRAM	38
P-CHG-02: CONFIGURATION CHANGE CONTROL	38
P-CHG-02.2: CONFIGURATION CHANGE CONTROL TEST, VALIDATE & DOCUMENT CHANGES	39
CLOUD SECURITY (CLD) PROCEDURES	40
P-CLD-01: CLOUD SERVICES	40
P-CLD-02: CLOUD SECURITY ARCHITECTURE	40
P-CLD-04: APPLICATION & PROGRAM INTERFACE (API) SECURITY	41
P-CLD-06: MULTI-TENANT ENVIRONMENTS	41
P-CLD-06.1: MULTI-TENANT ENVIRONMENTS CUSTOMER RESPONSIBILITY MATRIX (CRM)	42
P-CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS	42
COMPLIANCE (CPL) PROCEDURES	43
P-CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	43
P-CPL-01.1: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE NON-COMPLIANCE OVERSIGHT	43
P-CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE COMPLIANCE SCOPE	44
P-CPL-02: SECURITY & PRIVACY CONTROLS OVERSIGHT	44
P-CPL-02.1: SECURITY CONTROLS OVERSIGHT INTERNAL AUDIT FUNCTION	45
P-CPL-03: SECURITY ASSESSMENTS	46
P-CPL-03.1: SECURITY ASSESSMENTS INDEPENDENT ASSESSORS	46
P-CPL-03.2: SECURITY ASSESSMENTS FUNCTIONAL REVIEW OF SECURITY CONTROLS	47
P-CPL-04: AUDIT ACTIVITIES	47
CONFIGURATION MANAGEMENT (CFG) PROCEDURES	48
P-CFG-01: CONFIGURATION MANAGEMENT PROGRAM	48
P-CFG-01.1: CONFIGURATION MANAGEMENT PROGRAM ASSIGNMENT OF RESPONSIBILITY	48
P-CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS	49
P-CFG-02.1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS REVIEWS & UPDATES	50
P-CFG-02.4: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS DEVELOPMENT & TEST ENVIRONMENTS	51
P-CFG-02.5: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS	51
P-CFG-03: LEAST FUNCTIONALITY	51
P-CFG-03.1: LEAST FUNCTIONALITY PERIODIC REVIEW	52
CONTINUOUS MONITORING (MON) PROCEDURES	53
P-MON-01: CONTINUOUS MONITORING	53
P-MON-01.1: CONTINUOUS MONITORING INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)	54
P-MON-01.2: CONTINUOUS MONITORING AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	54
P-MON-01.3: CONTINUOUS MONITORING INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC	55
P-MON-01.4: CONTINUOUS MONITORING SYSTEM GENERATED ALERTS	55
P-MON-01.8: CONTINUOUS MONITORING REVIEWS & UPDATES	56
P-MON-02: CENTRALIZED EVENT LOG COLLECTION	56
P-MON-02.1: CENTRALIZED SECURITY EVENT LOG COLLECTION CORRELATE MONITORING INFORMATION	58
P-MON-02.2: CENTRALIZED SECURITY EVENT LOG COLLECTION CENTRAL REVIEW & ANALYSIS	58
P-MON-03: CONTENT OF AUDIT RECORDS	59
P-MON-03.3: CONTENT OF AUDIT RECORDS PRIVILEGED FUNCTIONS LOGGING	59
P-MON-06: MONITORING REPORTING	60
P-MON-08: PROTECTION OF EVENT LOGS	60
P-MON-11: MONITORING FOR INFORMATION DISCLOSURE	61
P-MON-11.3: MONITORING FOR INFORMATION DISCLOSURE MONITORING FOR INDICATORS OF COMPROMISE (IOC)	61
CRYPTOGRAPHIC PROTECTIONS (CRY) PROCEDURES	62
P-CRY-01: USE OF CRYPTOGRAPHIC CONTROLS	62

<i>P-CRY-01.2: USE OF CRYPTOGRAPHIC CONTROLS EXPORT-CONTROLLED TECHNOLOGY</i>	63
P-CRY-03: TRANSMISSION CONFIDENTIALITY	63
P-CRY-04: TRANSMISSION INTEGRITY	64
P-CRY-05: ENCRYPTING DATA AT REST	64
P-CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT	64
<i>P-CRY-09.3: CRYPTOGRAPHIC KEY MANAGEMENT CRYPTOGRAPHIC KEY LOSS OR CHANGE</i>	65
<i>P-CRY-09.4: CRYPTOGRAPHIC KEY MANAGEMENT CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS</i>	66
DATA CLASSIFICATION & HANDLING (DCH) PROCEDURES	67
P-DCH-01: DATA PROTECTION	67
P-DCH-02: DATA & ASSET CLASSIFICATION	67
P-DCH-03: MEDIA ACCESS	67
<i>P-DCH-03.2: MEDIA ACCESS MASKING DISPLAYED DATA</i>	68
P-DCH-04: MEDIA MARKING	69
P-DCH-06: MEDIA STORAGE	69
P-DCH-07: MEDIA TRANSPORTATION	69
<i>P-DCH-07.1: MEDIA TRANSPORTATION CUSTODIANS</i>	70
<i>P-DCH-07.2: MEDIA TRANSPORTATION ENCRYPTING DATA IN STORAGE MEDIA</i>	70
P-DCH-08: PHYSICAL MEDIA DISPOSAL	71
P-DCH-09: DIGITAL MEDIA SANITIZATION	71
<i>P-DCH-09.1: MEDIA SANITIZATION MEDIA SANITIZATION DOCUMENTATION</i>	72
<i>P-DCH-09.3: MEDIA SANITIZATION SANITIZATION OF PERSONAL DATA (PD)</i>	72
P-DCH-10: MEDIA USE	73
<i>P-DCH-10.1: MEDIA USE LIMITATIONS ON USE</i>	73
P-DCH-12: REMOVABLE MEDIA SECURITY	74
P-DCH-14: INFORMATION SHARING	74
P-DCH-17: AD-HOC TRANSFERS	74
P-DCH-18: MEDIA & DATA RETENTION	75
P-DCH-21: INFORMATION DISPOSAL	75
P-DCH-23: DE-IDENTIFICATION	76
<i>P-DCH-23.4: DE-IDENTIFICATION REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS</i>	76
ENDPOINT SECURITY (END) PROCEDURES	78
P-END-01: WORKSTATION SECURITY	78
P-END-02: ENDPOINT PROTECTION MEASURES	78
P-END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	79
<i>P-END-03.2: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS GOVERNING ACCESS RESTRICTION FOR CHANGE</i>	79
P-END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	80
<i>P-END-04.1: MALICIOUS CODE PROTECTION AUTOMATIC ANTIMALWARE SIGNATURE UPDATES</i>	80
HUMAN RESOURCES SECURITY (HRS) PROCEDURES	82
P-HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	82
P-HRS-02: POSITION CATEGORIZATION	82
P-HRS-03: ROLES & RESPONSIBILITIES	83
<i>P-HRS-03.1: ROLES & RESPONSIBILITIES USER AWARENESS</i>	83
<i>P-HRS-03.2: ROLES & RESPONSIBILITIES COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS</i>	84
P-HRS-04: PERSONNEL SCREENING	84
<i>P-HRS-04.1: PERSONNEL SCREENING ROLES WITH SPECIAL PROTECTION MEASURES</i>	85
<i>P-HRS-04.2: PERSONNEL SCREENING FORMAL INDOCTRINATION</i>	85
P-HRS-05: TERMS OF EMPLOYMENT	85
<i>P-HRS-05.1: TERMS OF EMPLOYMENT RULES OF BEHAVIOR</i>	86
<i>P-HRS-05.2: TERMS OF EMPLOYMENT SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS</i>	86
<i>P-HRS-05.3: TERMS OF EMPLOYMENT USE OF COMMUNICATIONS TECHNOLOGY</i>	87
<i>P-HRS-05.4: TERMS OF EMPLOYMENT USE OF CRITICAL TECHNOLOGIES</i>	87
<i>P-HRS-05.5: TERMS OF EMPLOYMENT USE OF MOBILE DEVICES</i>	88
<i>P-HRS-05.7: TERMS OF EMPLOYMENT POLICY FAMILIARIZATION & ACKNOWLEDGEMENT</i>	88
P-HRS-06: ACCESS AGREEMENTS	88
<i>P-HRS-06.1: ACCESS AGREEMENTS CONFIDENTIALITY AGREEMENTS</i>	89
P-HRS-07: PERSONNEL SANCTIONS	89
<i>P-HRS-07.1: PERSONNEL SANCTIONS WORKPLACE INVESTIGATIONS</i>	90

P-HRS-08: PERSONNEL TRANSFER	90
P-HRS-09: PERSONNEL TERMINATION	91
<i>P-HRS-09.3: PERSONNEL TERMINATION POST-EMPLOYMENT REQUIREMENTS</i>	91
P-HRS-11: SEPARATION OF DUTIES (SoD)	92
P-HRS-12: INCOMPATIBLE ROLES	92
<u>IDENTIFICATION & AUTHENTICATION (IAC) PROCEDURES</u>	<u>94</u>
P-IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	94
P-IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	94
P-IAC-03: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS	95
P-IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	95
P-IAC-05: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES	95
P-IAC-07: USER PROVISIONING & DE-PROVISIONING	96
<i>P-IAC-07.1: USER PROVISIONING & DE-PROVISIONING CHANGE OF ROLES & DUTIES</i>	96
<i>P-IAC-07.2: USER PROVISIONING & DE-PROVISIONING TERMINATION OF EMPLOYMENT</i>	97
P-IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	97
P-IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)	98
<i>P-IAC-09.1: IDENTIFIER MANAGEMENT USER IDENTITY (ID) MANAGEMENT</i>	99
<i>P-IAC-09.4: IDENTIFIER MANAGEMENT CROSS-ORGANIZATION MANAGEMENT</i>	99
P-IAC-10: AUTHENTICATOR MANAGEMENT	100
<i>P-IAC-10.1: AUTHENTICATOR MANAGEMENT PASSWORD-BASED AUTHENTICATION</i>	100
<i>P-IAC-10.5: AUTHENTICATOR MANAGEMENT PROTECTION OF AUTHENTICATORS</i>	102
<i>P-IAC-10.8: AUTHENTICATOR MANAGEMENT VENDOR-SUPPLIED DEFAULTS</i>	102
<i>P-IAC-10.11: AUTHENTICATOR MANAGEMENT PASSWORD MANAGERS</i>	102
P-IAC-15: ACCOUNT MANAGEMENT	103
<i>P-IAC-15.1: ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT</i>	104
<i>P-IAC-15.2: ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</i>	104
<i>P-IAC-15.3: ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS</i>	105
<i>P-IAC-15.5: ACCOUNT MANAGEMENT RESTRICTIONS ON SHARED GROUPS / ACCOUNTS</i>	105
P-IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)	105
<i>P-IAC-16.1: PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED ACCOUNT INVENTORIES</i>	106
P-IAC-17: PERIODIC REVIEW OF ACCOUNT PRIVILEGES	106
P-IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT	107
P-IAC-19: CREDENTIAL SHARING	107
P-IAC-20: ACCESS ENFORCEMENT	108
<i>P-IAC-20.1: ACCESS ENFORCEMENT ACCESS TO SENSITIVE DATA</i>	108
<i>P-IAC-20.2: ACCESS ENFORCEMENT DATABASE ACCESS</i>	109
<i>P-IAC-20.3: ACCESS ENFORCEMENT USE OF PRIVILEGED UTILITY PROGRAMS</i>	109
P-IAC-21: LEAST PRIVILEGE	110
<i>P-IAC-21.3: LEAST PRIVILEGE PRIVILEGED ACCOUNTS</i>	110
P-IAC-22: ACCOUNT LOCKOUT	111
<u>INCIDENT RESPONSE (IRO) PROCEDURES</u>	<u>112</u>
P-IRO-01: INCIDENTS RESPONSE OPERATIONS	112
P-IRO-02: INCIDENT HANDLING	112
P-IRO-04: INCIDENT RESPONSE PLAN (IRP)	113
<i>P-IRO-04.1: INCIDENT RESPONSE PLAN (IRP) DATA BREACH</i>	113
P-IRO-05: INCIDENT RESPONSE TRAINING	114
P-IRO-06: INCIDENT RESPONSE TESTING	114
<i>P-IRO-06.1: INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS</i>	114
P-IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)	115
P-IRO-08: CHAIN OF CUSTODY & FORENSICS	115
P-IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS	116
P-IRO-10: INCIDENT STAKEHOLDER REPORTING	116
<i>P-IRO-10.3: INCIDENT REPORTING VULNERABILITIES RELATED TO INCIDENTS</i>	117
<i>P-IRO-10.4: INCIDENT REPORTING SUPPLY CHAIN COORDINATION</i>	117
P-IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	118
<u>INFORMATION ASSURANCE (IAO) PROCEDURES</u>	<u>120</u>
P-IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS	120

P-IAO-02: ASSESSMENTS	120
<i>P-IAO-02.2: ASSESSMENTS SPECIALIZED ASSESSMENTS</i>	121
P-IAO-04: THREAT ANALYSIS & FLAW REMEDIATION DURING DEVELOPMENT	122
<u>MAINTENANCE (MNT) PROCEDURES</u>	<u>123</u>
P-MNT-01: MAINTENANCE OPERATIONS	123
P-MNT-02: CONTROLLED MAINTENANCE	123
P-MNT-03: TIMELY MAINTENANCE	124
<u>MOBILE DEVICE MANAGEMENT (MDM) PROCEDURES</u>	<u>125</u>
P-MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES	125
P-MDM-02: ACCESS CONTROL FOR MOBILE DEVICES	125
P-MDM-05: REMOTE PURGING	126
<u>NETWORK SECURITY (NET) PROCEDURES</u>	<u>127</u>
P-NET-01: NETWORK SECURITY CONTROLS (NSC)	127
P-NET-02: LAYERED DEFENSES	127
P-NET-03: BOUNDARY PROTECTION	128
P-NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)	129
<i>P-NET-04.1: DATA FLOW ENFORCEMENT DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION</i>	130
P-NET-06: NETWORK SEGMENTATION	130
<i>P-NET-06.1: SECURITY FUNCTION ISOLATION SECURITY MANAGEMENT SUBNETS</i>	131
P-NET-08: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS / NIPS)	132
<i>P-NET-08.1: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS / NIPS) DMZ NETWORKS</i>	132
P-NET-13: ELECTRONIC MESSAGING	133
P-NET-14: REMOTE ACCESS	133
<i>P-NET-14.5: REMOTE ACCESS WORK FROM ANYWHERE (WFA) – TELECOMMUTING SECURITY</i>	134
P-NET-15: WIRELESS NETWORKING	134
P-NET-18: DNS & CONTENT FILTERING	135
<u>PHYSICAL & ENVIRONMENTAL SECURITY (PES) PROCEDURES</u>	<u>136</u>
P-PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS	136
P-PES-02: PHYSICAL ACCESS AUTHORIZATIONS	136
<i>P-PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS ROLE-BASED PHYSICAL ACCESS</i>	137
P-PES-03: PHYSICAL ACCESS CONTROL	137
<i>P-PES-03.1: PHYSICAL ACCESS CONTROL CONTROLLED INGRESS & EGRESS POINTS</i>	138
<i>P-PES-03.3: PHYSICAL ACCESS CONTROL PHYSICAL ACCESS LOGS</i>	138
P-PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES	139
<i>P-PES-04.1: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES WORKING IN SECURE AREAS</i>	139
P-PES-05: MONITORING PHYSICAL ACCESS	140
<i>P-PES-05.1: MONITORING PHYSICAL ACCESS INTRUSION ALARMS / SURVEILLANCE EQUIPMENT</i>	140
<i>P-PES-05.2: MONITORING PHYSICAL ACCESS MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS</i>	141
P-PES-06: VISITOR CONTROL	141
P-PES-07: SUPPORTING UTILITIES	142
<i>P-PES-07.1: SUPPORTING UTILITIES AUTOMATIC VOLTAGE CONTROLS</i>	142
<i>P-PES-07.2: SUPPORTING UTILITIES EMERGENCY SHUTOFF</i>	142
<i>P-PES-07.3: SUPPORTING UTILITIES EMERGENCY POWER</i>	143
<i>P-PES-07.4: SUPPORTING UTILITIES EMERGENCY LIGHTING</i>	143
P-PES-10: DELIVERY & REMOVAL	143
P-PES-12: EQUIPMENT SITING & PROTECTION	144
<i>P-PES-12.1: EQUIPMENT SITING & PROTECTION TRANSMISSION MEDIUM SECURITY</i>	144
P-PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS	145
<u>PRIVACY (PRI) PROCEDURES</u>	<u>146</u>
P-PRI-01: PRIVACY PROGRAM	146
<i>P-PRI-01.3: PRIVACY PROGRAM DISSEMINATION OF PRIVACY PROGRAM INFORMATION</i>	146
<i>P-PRI-01.6: PRIVACY PROGRAM SECURITY OF PERSONAL DATA</i>	147
P-PRI-02: PRIVACY NOTICE	147
<i>P-PRI-02.1: PRIVACY NOTICE PURPOSE SPECIFICATION</i>	148
P-PRI-03: CHOICE & CONSENT	148
P-PRI-04: RESTRICT COLLECTION TO IDENTIFIED PURPOSE	148

P-PRI-05: PERSONAL DATA RETENTION & DISPOSAL	149
<i>P-PRI-05.1: USE, RETENTION & DISPOSAL INTERNAL USE OF PERSONAL DATA FOR TESTING, TRAINING AND RESEARCH</i>	149
<i>P-PRI-05.3: USE, RETENTION & DISPOSAL DATA MASKING</i>	150
<i>P-PRI-05.4: USE, RETENTION & DISPOSAL USAGE RESTRICTIONS OF SENSITIVE PERSONAL DATA</i>	150
P-PRI-07: INFORMATION SHARING WITH THIRD PARTIES	150
<i>P-PRI-07.1: INFORMATION SHARING WITH THIRD PARTIES PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS</i>	151
P-PRI-08: TESTING, TRAINING & MONITORING	151
PROJECT & RESOURCE MANAGEMENT (PRM) PROCEDURES	153
P-PRM-01: SECURITY PORTFOLIO MANAGEMENT	153
P-PRM-02: SECURITY & PRIVACY RESOURCE MANAGEMENT	153
P-PRM-03: ALLOCATION OF RESOURCES	153
P-PRM-04: SECURITY & PRIVACY IN PROJECT MANAGEMENT	154
P-PRM-05: SECURITY & PRIVACY REQUIREMENTS DEFINITION	154
P-PRM-07: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT	155
RISK MANAGEMENT (RSK) PROCEDURES	156
P-RSK-01: RISK MANAGEMENT PROGRAM	156
<i>P-RSK-01.1: RISK MANAGEMENT PROGRAM (RMP) RISK FRAMING</i>	156
P-RSK-02: RISK-BASED SECURITY CATEGORIZATION	157
P-RSK-03: RISK IDENTIFICATION	157
P-RSK-04: RISK ASSESSMENT	157
<i>P-RSK-04.1: RISK ASSESSMENT RISK REGISTER</i>	158
P-RSK-05: RISK RANKING	159
P-RSK-06: RISK REMEDIATION	159
<i>P-RSK-06.1: RISK REMEDIATION RISK RESPONSE</i>	159
P-RSK-07: RISK ASSESSMENT UPDATE	160
P-RSK-08: BUSINESS IMPACT ANALYSIS (BIA)	160
P-RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN	161
<i>P-RSK-09.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN SUPPLY CHAIN RISK ASSESSMENT</i>	161
P-RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)	162
SECURE ENGINEERING & ARCHITECTURE (SEA) PROCEDURES	163
P-SEA-01: SECURE ENGINEERING PRINCIPLES	163
<i>P-SEA-01.1: SECURE ENGINEERING PRINCIPLES CENTRALIZED MANAGEMENT OF CYBERSECURITY & PRIVACY CONTROLS</i>	164
P-SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE	164
<i>P-SEA-02.1: ALIGNMENT WITH ENTERPRISE ARCHITECTURE STANDARDIZED TERMINOLOGY</i>	165
P-SEA-17: SECURE LOG-ON PROCEDURES	165
P-SEA-20: CLOCK SYNCHRONIZATION	165
SECURITY OPERATIONS (OPS) PROCEDURES	167
P-OPS-01: OPERATIONS SECURITY	167
<i>P-OPS-01.1: OPERATIONS SECURITY STANDARDIZED OPERATING PROCEDURES (SOP)</i>	167
P-OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)	168
P-OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)	169
SECURITY AWARENESS & TRAINING (SAT) PROCEDURES	170
P-SAT-01: SECURITY & PRIVACY-MINDED WORKFORCE	170
P-SAT-02: SECURITY & PRIVACY AWARENESS	170
P-SAT-03: ROLE-BASED SECURITY & PRIVACY TRAINING	171
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) PROCEDURES	173
P-TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION	173
P-TDA-02: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS	173
<i>P-TDA-02.3: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS DEVELOPMENT METHODS, TECHNIQUES & PROCESSES</i>	173
P-TDA-05: DEVELOPER ARCHITECTURE & DESIGN	174
P-TDA-06: SECURE CODING	175
<i>P-TDA-06.1: SECURE CODING CRITICALITY ANALYSIS</i>	175
P-TDA-07: SECURE DEVELOPMENT ENVIRONMENTS	176
P-TDA-08: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS	176

P-TDA-09: SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT	177
P-TDA-10: USE OF LIVE DATA	177
P-TDA-14: DEVELOPER CONFIGURATION MANAGEMENT	178
P-TDA-15: DEVELOPER THREAT ANALYSIS & FLAW REMEDIATION	178
P-TDA-20: ACCESS TO PROGRAM SOURCE CODE	179
THIRD-PARTY MANAGEMENT (TPM) PROCEDURES	180
P-TPM-01: THIRD-PARTY MANAGEMENT	180
<i>P-TPM-01.1: THIRD-PARTY MANAGEMENT THIRD-PARTY INVENTORIES</i>	180
P-TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS	181
P-TPM-03: SUPPLY CHAIN PROTECTION	181
<i>P-TPM-03.1: SUPPLY CHAIN PROTECTION ACQUISITION STRATEGIES, TOOLS & METHODS</i>	181
<i>P-TPM-03.2: SUPPLY CHAIN PROTECTION LIMIT POTENTIAL HARM</i>	182
<i>P-TPM-03.3: SUPPLY CHAIN PROTECTION PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES</i>	182
P-TPM-04: THIRD-PARTY SERVICES	183
<i>P-TPM-04.1: THIRD-PARTY SERVICES THIRD-PARTY RISK ASSESSMENTS & APPROVALS</i>	183
<i>P-TPM-04.3: THIRD-PARTY SERVICES CONFLICT OF INTERESTS</i>	184
<i>P-TPM-04.4: THIRD-PARTY SERVICES THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS</i>	184
P-TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	184
<i>P-TPM-05.1: THIRD-PARTY CONTRACT REQUIREMENTS SECURITY COMPROMISE NOTIFICATION AGREEMENTS</i>	185
<i>P-TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX</i>	185
P-TPM-06: THIRD-PARTY PERSONNEL SECURITY	186
P-TPM-08: REVIEW OF THIRD-PARTY SERVICES	186
P-TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION	187
P-TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES	187
P-TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	187
THREAT MANAGEMENT (THR) PROCEDURES	189
P-THR-01: THREAT AWARENESS PROGRAM	189
P-THR-02: INDICATORS OF EXPOSURE (IOE)	189
P-THR-03: THREAT INTELLIGENCE FEEDS	189
VULNERABILITY & PATCH MANAGEMENT (VPM) PROCEDURES	191
P-VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	191
<i>P-VPM-01.1: VULNERABILITY & PATCH MANAGEMENT PROGRAM ATTACK SURFACE SCOPE</i>	191
P-VPM-02: VULNERABILITY REMEDIATION PROCESS	191
P-VPM-03: VULNERABILITY RANKING	192
P-VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES	192
<i>P-VPM-04.2: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES FLAW REMEDIATION WITH PERSONAL DATA (PD)</i>	193
P-VPM-05: SOFTWARE & FIRMWARE PATCHING	193
P-VPM-06: VULNERABILITY SCANNING	194
WEB SECURITY (WEB) PROCEDURES	196
P-WEB-02: USE OF DEMILITARIZED ZONES (DMZ)	196
GLOSSARY: ACRONYMS & DEFINITIONS	197
ACRONYMS	197
DEFINITIONS	197
RECORD OF CHANGES	198

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).

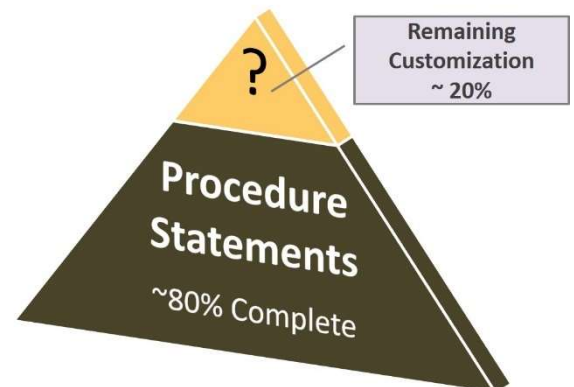
OVERVIEW

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 reassess 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 cybersecurity program, since procedures represents the specific activities that are performed to protect systems and data.

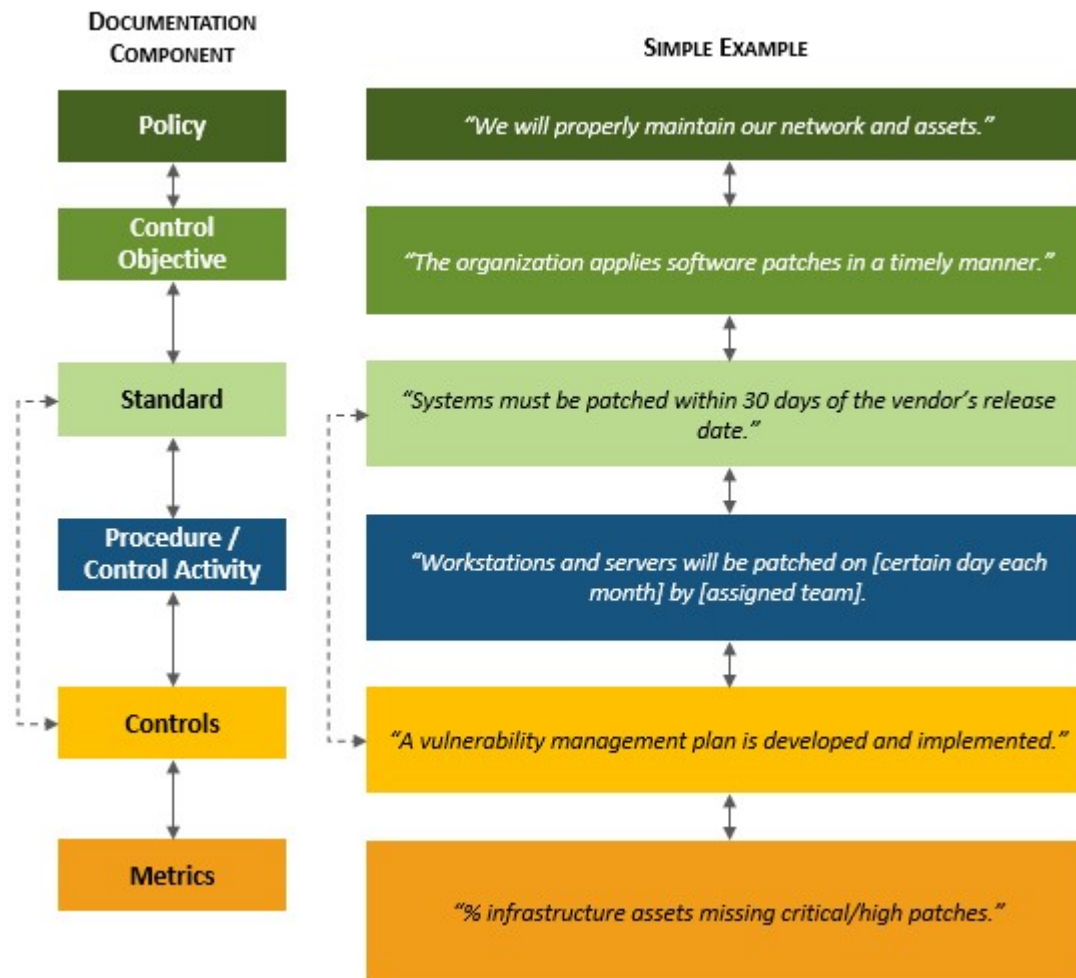
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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!



NIST NICE Cybersecurity Workforce Framework – Work Categories

EXAMPLE

This example is a configuration procedure **P-CFG-02 (System Hardening Through Baseline 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*

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

Control: Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards. *[control wording comes directly from the Secure Controls Framework (SCF) control #CFG-02. The SCF is a free resource that can be downloaded from <https://www.securecontrolsframework.com>]*

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 that enable the implementation of appropriate physical, administrative and technical mechanisms to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory, and regulatory compliance obligations.
- (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.

CYBERSECURITY & PRIVACY GOVERNANCE (GOV) PROCEDURES

Management Intent: The purpose of the Cybersecurity Governance (GOV) procedures / control activities is to specify the development, proactive management and ongoing review of ACME's cybersecurity and privacy program.

P-GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control: Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.

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) Develops an organization-wide digital security governance program to provide complete coverage for all cybersecurity and privacy-related controls needed to address statutory, regulatory and contractual obligations, as well as to address possible threats to data and or assets.
- (2) Documents the ACME digital security governance program in a single document, the Digital Security Program (DSP).
- (3) 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.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-GOV-01.1: DIGITAL SECURITY GOVERNANCE PROGRAM | STEERING COMMITTEE

Control: Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001]:

- (1) Develops a steering committee to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives.
- (2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, privacy and business executives).
- (3) Assigns roles to steering committee personnel:
 - a. Chair;
 - b. Vice Chair; and
 - c. Committee Staff;
- (4) Defines the expected conduct the steering committee meetings to ensure cybersecurity and privacy solutions and services follows the CARES principles:
 - a. Competitive in scope and price over the long term;
 - b. Adaptable and customized to meet stakeholder needs;
 - c. Resolute in delivering timely solutions that address present and emerging risks;
 - d. Equitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
 - e. Stable in supporting cost-effective, fiscally-prudent operations and in building long-term relationships with stakeholders and program/service partners.
- (5) Requires steering committee members to attend each steering committee meeting or send a representative.
- (6) Requires the steering committee to keeps and prepare meeting minutes for review and approval.
- (7) Requires the steering committee to meet at least quarterly (in-person or teleconference).
- (8) Requires a quorum of committee members to hold a meeting;
- (9) Governs the review of cybersecurity and privacy-related projects/initiatives accordingly:
 - a. Each project must be assigned a sponsor, typically from the submitting department;
 - b. Projects must be presented in writing to the Committee Chair and will contain a business case of adequate detail to allow the steering committee to assess and prioritize the work and shall include cost and personnel resource estimates as well as funding sources;
 - c. The Committee Chair must review the submission for completeness and accuracy prior to setting the submission on an agenda;
 - d. Submissions must be distributed electronically to members of the steering committee prior to the agenda date;

- e. The project sponsor may be asked to make a presentation to the steering committee on the project at the steering committee meeting; and
 - f. The steering committee must review and discuss the submission and accept a motion from the steering committee to take one of the following actions:
 - i. Approve the project;
 - ii. Return the project to the department for revision or further information;
 - iii. Table the project for later action;
 - iv. Deny the project; or
 - v. Other action as suggested in the motion.
- (10) A simple majority vote of the committee members present is required for an affirmative vote. In the event of a tie vote, at the discretion of the Committee Chair, one of the following options may be used:
- a. Resolve the impasse by further discussion and calling for an additional vote; or
 - b. Send the submission back for further analysis, clarification or revision.
- (11) 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.
- (12) If necessary, requests corrective action to address identified deficiencies.
- (13) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (14) If necessary, documents the results of corrective action and notes findings.
- (15) If necessary, requests additional corrective action to address unremediated deficiencies.

P-GOV-01.2: DIGITAL SECURITY GOVERNANCE PROGRAM | STATUS REPORTING TO GOVERNING BODY

Control: Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program.

Procedure / Control Activity: Executive Cyber Leadership [OV-EXL-001]:

- (1) Develops a steering committee to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives.
- (2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, privacy and business executives).
- (3) Assigns roles to steering committee personnel:
 - a. Chair;
 - b. Vice Chair; and
 - c. Committee Staff;
- (4) Defines the expected conduct the steering committee meetings to ensure cybersecurity and privacy solutions and services follows the CARES principles:
 - a. Competitive in scope and price over the long term;
 - b. Adaptable and customized to meet stakeholder needs;
 - c. Resolute in delivering timely solutions that address present and emerging risks;
 - d. Equitable in allocating costs and services between various stakeholders in a fair and consistent manner; and
 - e. Stable in supporting cost-effective, fiscally-prudent operations and in building long-term relationships with stakeholders and program/service partners.
- (5) Requires steering committee members to attend each steering committee meeting or send a representative.
- (6) Requires the steering committee to keep and prepare meeting minutes for review and approval.
- (7) Requires the steering committee to meet at least quarterly (in-person or teleconference).
- (8) Requires a quorum of committee members to hold a meeting;
- (9) Governs the review of cybersecurity and privacy-related projects/initiatives accordingly:
 - a. Each project must be assigned a sponsor, typically from the submitting department;
 - b. Projects must be presented in writing to the Committee Chair and will contain a business case of adequate detail to allow the steering committee to assess and prioritize the work and shall include cost and personnel resource estimates as well as funding sources;
 - c. The Committee Chair must review the submission for completeness and accuracy prior to setting the submission on an agenda;
 - d. Submissions must be distributed electronically to members of the steering committee prior to the agenda date;
 - e. The project sponsor may be asked to make a presentation to the steering committee on the project at the steering committee meeting; and

CHANGE MANAGEMENT (CHG) PROCEDURES

Management Intent: The purpose of the Change Management (CHG) procedures / control activities is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

P-CHG-01: CHANGE MANAGEMENT PROGRAM

Control: Mechanisms exist to facilitate the implementation of a change management program.

Procedure / Control Activity: Change Control Manager [XX-CHG-001], in conjunction with Systems Security Manager [OV-MGT-001] and Executive Cyber Leadership [OV-EXL-001]:

- (1) Develops, implements and governs controls that are sufficient for managing and documenting change management activities that includes:
 - a. A formal, documented change management program; and
 - b. Processes to facilitate the implementation of changes.
- (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.

P-CHG-02: CONFIGURATION CHANGE CONTROL

Control: Mechanisms exist to govern the technical configuration change control processes.

Procedure / Control Activity: Change Control Manager [XX-CHG-001], in conjunction with Systems Security Manager [OV-MGT-001] and Executive Cyber Leadership [OV-EXL-001]:

- (1) Develops, implements and governs controls that are sufficient for managing and documenting change management activities that includes:
 - a. A formal, documented change management program; and
 - b. Processes to facilitate the implementation of changes, where changes are:
 - i. Tracked;⁸
 - ii. Reviewed;⁹
 - iii. Approved or Disapproved;¹⁰ and
 - iv. Documented.¹¹
- (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.

⁸ NIST SP 800-171A / CMMC assessment criteria 3.4.3[a] / CM.L2-3.4.3[a]

⁹ NIST SP 800-171A / CMMC assessment criteria 3.4.3[b] / CM.L2-3.4.3[b]

¹⁰ NIST SP 800-171A / CMMC assessment criteria 3.4.3[c] / CM.L2-3.4.3[c]

¹¹ NIST SP 800-171A / CMMC assessment criteria 3.4.3[d] / CM.L2-3.4.3[d]

P-CHG-02.2: CONFIGURATION CHANGE CONTROL | TEST, VALIDATE & DOCUMENT CHANGES

Control: Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.

Procedure / Control Activity: Change Control Manager [XX-CHG-001]:

- (1) Implements appropriate administrative and technical means to ensure asset owner and custodians:
 - a. Test and validate configuration changes in a test environment, prior to deploying the change in the production environment; and
 - b. Review and test systems, applications and processes to ensure there is no adverse impact on organizational operations or security when major upgrades/updates are applied.
- (2) If it is not technically or logistically feasible to test a configuration change, identifies compensating controls to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include:
 - a. Images of systems;
 - b. Backups of configurations;
 - c. Viable back out plan; and/or
 - d. After-hours implementation.
- (3) 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.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

THIRD-PARTY MANAGEMENT (TPM) PROCEDURES

Management Intent: The purpose of the Third-Party Management (TPM) procedures / control activities is to ensure that risk associated with third-parties are minimized or avoided.

P-TPM-01: THIRD-PARTY MANAGEMENT

Control: Mechanisms exist to facilitate the implementation of third-party management controls.

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

- (1) Uses vendor-recommended settings and industry-recognized secure practices to ensure controls are sufficient for managing third-party service providers' compliance with cybersecurity, privacy and service delivery requirements included in third-party contracts by:
 - a. Requiring data/process owners maintain and implement procedures to manage service providers that includes:
 - i. Maintaining a list of service providers;
 - ii. Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of sensitive/regulated data the service providers possess or otherwise store, process or transmit on behalf of ACME, or to the extent that they could impact the security of ACME;
 - iii. Monitoring and ensuring there is an established process for engaging service providers, including proper due diligence prior to engagement;
 - iv. Maintaining a program to monitor service providers' compliance status at least annually; and
 - v. Maintaining information about which requirements are managed by each service provider, and which are managed by ACME.
 - b. Utilizing the process of due diligence:
 - i. Direct observations;
 - ii. Reviews of policies and procedures; and
 - iii. Reviews of supporting documentation.
- (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.

P-TPM-01.1: THIRD-PARTY MANAGEMENT | THIRD-PARTY INVENTORIES

Control: Mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.

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

- (1) Uses Implements appropriate administrative and technical means to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of ACME' technology assets and data.
- (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.