

YOUR LOGO GOES HERE

CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

NIST CYBERSECURITY FRAMEWORK 2.0

ACME Consulting Partners, LLP

SENSITIVE

Access Limited to Authorized Personnel

TABLE OF CONTENTS

OVERVIEW, INSTRUCTIONS & EXAMPLE	8
KEY TERMINOLOGY	8
OVERVIEW	8
<i>CUSTOMIZATION GUIDANCE</i>	<i>ERROR! BOOKMARK NOT DEFINED.</i>
<i>VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES</i>	<i>8</i>
PROCEDURES DOCUMENTATION	9
NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK	10
EXAMPLE	10
SUPPORTING POLICIES & STANDARDS	12
KNOWN COMPLIANCE REQUIREMENTS	14
STATUTORY REQUIREMENTS	14
REGULATORY REQUIREMENTS	14
CONTRACTUAL REQUIREMENTS	14
CYBERSECURITY & DATA PROTECTION GOVERNANCE (GOV) PROCEDURES	15
P-GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM	15
<i>P-GOV-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM STEERING COMMITTEE & PROGRAM OVERSIGHT</i>	<i>15</i>
<i>P-GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM STATUS REPORTING TO GOVERNING BODY</i>	<i>16</i>
P-GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION	17
<i>P-GOV-02.1: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION EXCEPTION MANAGEMENT</i>	<i>18</i>
P-GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY & DATA PROTECTION PROGRAM	18
P-GOV-04: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES	19
<i>P-GOV-04.1: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES ACCOUNTABILITY STRUCTURE</i>	<i>19</i>
P-GOV-05: MEASURES OF PERFORMANCE	20
<i>P-GOV-05.2: MEASURES OF PERFORMANCE KEY RISK INDICATORS (KRIS)</i>	<i>20</i>
P-GOV-07: CONTACTS WITH GROUPS & ASSOCIATIONS	20
P-GOV-08: DEFINED BUSINESS CONTEXT & MISSION	21
P-GOV-09: DEFINED CONTROL OBJECTIVES	21
P-GOV-16: MATERIALITY DETERMINATION	22
ASSET MANAGEMENT (AST) PROCEDURES	23
P-AST-01: ASSET GOVERNANCE	23
<i>P-AST-01.1: ASSET GOVERNANCE ASSET-SERVICE DEPENDENCIES</i>	<i>23</i>
<i>P-AST-01.2: ASSET GOVERNANCE STAKEHOLDER IDENTIFICATION & INVOLVEMENT</i>	<i>24</i>
P-AST-02: ASSET INVENTORIES	24
P-AST-03: ASSET OWNERSHIP ASSIGNMENT	25
<i>P-AST-03.1: ASSET OWNERSHIP ASSIGNMENT ACCOUNTABILITY INFORMATION</i>	<i>25</i>
P-AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	26
<i>P-AST-04.1: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) ASSET SCOPE CLASSIFICATION</i>	<i>26</i>
<i>P-AST-04.2: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) CONTROL APPLICABILITY BOUNDARY GRAPHICAL REPRESENTATION</i>	<i>27</i>
P-AST-15: TAMPER PROTECTION	28
P-AST-18: ROOTS OF TRUST PROTECTION	28
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) PROCEDURES	30
P-BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	30
<i>P-BCD-01.1: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH RELATED PLANS</i>	<i>30</i>
<i>P-BCD-01.2: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH EXTERNAL SERVICE PROVIDERS</i>	<i>31</i>
<i>P-BCD-01.4: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY TIME/POINT OBJECTIVES (RTO/RPO)</i>	<i>31</i>
<i>P-BCD-01.5: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY OPERATIONS CRITERIA</i>	<i>31</i>
<i>P-BCD-01.6: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY OPERATIONS COMMUNICATIONS</i>	<i>32</i>
P-BCD-02: IDENTIFY CRITICAL ASSETS	32
<i>P-BCD-02.1: IDENTIFY CRITICAL ASSETS RESUME ALL MISSIONS & BUSINESS FUNCTIONS</i>	<i>33</i>
P-BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	33
P-BCD-06: CONTINGENCY PLANNING & UPDATES	34
P-BCD-11: DATA BACKUPS	34
<i>P-BCD-11.1: DATA BACKUPS TESTING FOR RELIABILITY & INTEGRITY</i>	<i>35</i>
<i>P-BCD-11.5: DATA BACKUPS TEST RESTORATION USING SAMPLING</i>	<i>35</i>

<i>P-BCD-11.6: DATA BACKUPS TRANSFER TO ALTERNATE STORAGE SITE</i>	36
P-BCD-12: INFORMATION SYSTEM RECOVERY & RECONSTITUTION	36
P-BCD-13: BACKUP & RESTORATION HARDWARE PROTECTION	36
<i>P-BCD-13.1: BACKUP & RESTORATION HARDWARE PROTECTION RESTORATION INTEGRITY VERIFICATION</i>	37
CAPACITY & PERFORMANCE PLANNING (CAP) PROCEDURES	38
P-CAP-01: CAPACITY & PERFORMANCE MANAGEMENT	38
P-CAP-02: RESOURCE PRIORITY	38
P-CAP-03: CAPACITY PLANNING	38
P-CAP-04: PERFORMANCE MONITORING	39
P-CAP-05: ELASTIC EXPANSION	39
CHANGE MANAGEMENT (CHG) PROCEDURES	40
P-CHG-01: CHANGE MANAGEMENT PROGRAM	40
P-CHG-02: CONFIGURATION CHANGE CONTROL	40
<i>P-CHG-02.1: CONFIGURATION CHANGE CONTROL PROHIBITION OF CHANGES</i>	41
<i>P-CHG-02.2: CONFIGURATION CHANGE CONTROL TEST, VALIDATE & DOCUMENT CHANGES</i>	41
P-CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES	42
P-CHG-04: ACCESS RESTRICTION FOR CHANGE	42
COMPLIANCE (CPL) PROCEDURES	44
P-CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	44
<i>P-CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE COMPLIANCE SCOPE</i>	44
P-CPL-02: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT	45
P-CPL-03: CYBERSECURITY & DATA PROTECTION ASSESSMENTS	46
<i>P-CPL-03.2: CYBERSECURITY & DATA PROTECTION ASSESSMENTS FUNCTIONAL REVIEW OF CYBERSECURITY & DATA PROTECTION CONTROLS</i>	47
CONFIGURATION MANAGEMENT (CFG) PROCEDURES	48
P-CFG-01: CONFIGURATION MANAGEMENT PROGRAM	48
P-CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS	48
<i>P-CFG-02.1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS REVIEWS & UPDATES</i>	50
<i>P-CFG-02.5: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS</i>	51
P-CFG-03: LEAST FUNCTIONALITY	52
<i>P-CFG-03.2: LEAST FUNCTIONALITY PREVENT UNAUTHORIZED SOFTWARE EXECUTION</i>	53
P-CFG-05: USER-INSTALLED SOFTWARE	53
CONTINUOUS MONITORING (MON) PROCEDURES	55
P-MON-01: CONTINUOUS MONITORING	55
<i>P-MON-01.1: CONTINUOUS MONITORING INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)</i>	56
<i>P-MON-01.3: CONTINUOUS MONITORING INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC</i>	57
<i>P-MON-01.4: CONTINUOUS MONITORING SYSTEM GENERATED ALERTS</i>	57
<i>P-MON-01.7: CONTINUOUS MONITORING FILE INTEGRITY MONITORING (FIM)</i>	58
<i>P-MON-01.8: CONTINUOUS MONITORING REVIEWS & UPDATES</i>	58
<i>P-MON-01.12: CONTINUOUS MONITORING AUTOMATED ALERTS</i>	59
P-MON-02: CENTRALIZED EVENT LOG COLLECTION	60
<i>P-MON-02.1: CENTRALIZED SECURITY EVENT LOG COLLECTION CORRELATE MONITORING INFORMATION</i>	62
P-MON-03: CONTENT OF EVENT LOGS	62
P-MON-11: MONITORING FOR INFORMATION DISCLOSURE	63
<i>P-MON-11.3: MONITORING FOR INFORMATION DISCLOSURE MONITORING FOR INDICATORS OF COMPROMISE (IOC)</i>	63
P-MON-16: ANOMALOUS BEHAVIOR	64
<i>P-MON-16.1: ANOMALOUS BEHAVIOR INSIDER THREATS</i>	64
<i>P-MON-16.2: ANOMALOUS BEHAVIOR THIRD-PARTY THREATS</i>	65
<i>P-MON-16.3: ANOMALOUS BEHAVIOR UNAUTHORIZED ACTIVITIES</i>	65
<i>P-MON-16.4: ANOMALOUS BEHAVIOR ACCOUNT CREATION AND MODIFICATION LOGGING</i>	65
CRYPTOGRAPHIC PROTECTIONS (CRY) PROCEDURES	67
P-CRY-01: USE OF CRYPTOGRAPHIC CONTROLS	67
<i>P-CRY-01.1: USE OF CRYPTOGRAPHIC CONTROLS ALTERNATE PHYSICAL PROTECTION</i>	68
P-CRY-03: TRANSMISSION CONFIDENTIALITY	68
P-CRY-04: TRANSMISSION INTEGRITY	69

P-CRY-05: ENCRYPTING DATA AT REST	69
DATA CLASSIFICATION & HANDLING (DCH) PROCEDURES	71
P-DCH-01: DATA PROTECTION	71
<i>P-DCH-01.1: DATA PROTECTION DATA STEWARDSHIP</i>	71
<i>P-DCH-01.2: DATA PROTECTION SENSITIVE/REGULATED DATA PROTECTION</i>	71
<i>P-DCH-01.3: DATA PROTECTION SENSITIVE / REGULATED MEDIA RECORDS</i>	72
<i>P-DCH-01.4: DATA PROTECTION DEFINING ACCESS AUTHORIZATIONS FOR SENSITIVE / REGULATED DATA</i>	72
P-DCH-02: DATA & ASSET CLASSIFICATION	73
P-DCH-03: MEDIA ACCESS	73
P-DCH-06: MEDIA STORAGE	74
<i>P-DCH-06.2: MEDIA STORAGE SENSITIVE DATA INVENTORIES</i>	75
<i>P-DCH-06.3: MEDIA STORAGE PERIODIC SCANS FOR SENSITIVE DATA</i>	75
P-DCH-19: GEOGRAPHIC LOCATION OF DATA	76
ENDPOINT SECURITY (END) PROCEDURES	77
P-END-01: ENDPOINT SECURITY	77
P-END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	77
P-END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	78
P-END-06: ENDPOINT FILE INTEGRITY MONITORING (FIM)	79
HUMAN RESOURCES SECURITY (HRS) PROCEDURES	80
P-HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	80
P-HRS-02: POSITION CATEGORIZATION	81
P-HRS-03: ROLES & RESPONSIBILITIES	81
<i>P-HRS-03.1: ROLES & RESPONSIBILITIES USER AWARENESS</i>	82
P-HRS-05: TERMS OF EMPLOYMENT	82
<i>P-HRS-05.1: TERMS OF EMPLOYMENT RULES OF BEHAVIOR</i>	83
<i>P-HRS-05.7: TERMS OF EMPLOYMENT POLICY FAMILIARIZATION & ACKNOWLEDGEMENT</i>	84
P-HRS-07: PERSONNEL SANCTIONS	84
P-HRS-11: SEPARATION OF DUTIES (SOD)	84
IDENTIFICATION & AUTHENTICATION (IAC) PROCEDURES	86
P-IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	86
<i>P-IAC-01.2: IDENTITY & ACCESS MANAGEMENT (IAM) AUTHENTICATE, AUTHORIZE AND AUDIT (AAA)</i>	86
P-IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	87
<i>P-IAC-02.2: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS REPLAY-RESISTANT AUTHENTICATION</i>	87
P-IAC-03: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS	88
<i>P-IAC-03.5: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF EXTERNAL AUTHENTICATORS</i>	88
P-IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	88
P-IAC-05: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES	89
P-IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	89
P-IAC-21: LEAST PRIVILEGE	90
P-IAC-28: IDENTITY PROOFING (IDENTITY VERIFICATION)	90
INCIDENT RESPONSE (IRO) PROCEDURES	92
P-IRO-01: INCIDENTS RESPONSE OPERATIONS	92
P-IRO-02: INCIDENT HANDLING	92
<i>P-IRO-02.4: INCIDENT HANDLING INCIDENT CLASSIFICATION & PRIORITIZATION</i>	93
<i>P-IRO-02.5: INCIDENT HANDLING CORRELATION WITH EXTERNAL ORGANIZATIONS</i>	94
P-IRO-03: INDICATORS OF COMPROMISE (IOC)	95
P-IRO-04: INCIDENT RESPONSE PLAN (IRP)	95
<i>P-IRO-04.2: INCIDENT RESPONSE PLAN (IRP) IRP UPDATE</i>	96
P-IRO-06: INCIDENT RESPONSE TESTING	96
<i>P-IRO-06.1: INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS</i>	97
P-IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)	97
P-IRO-08: CHAIN OF CUSTODY & FORENSICS	98
P-IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS	98
P-IRO-10: INCIDENT STAKEHOLDER REPORTING	99
<i>P-IRO-10.2: INCIDENT STAKEHOLDER REPORTING CYBER INCIDENT REPORTING FOR COVERED DEFENSE INFORMATION (CDI)</i>	100

<i>P-IRO-10.4: INCIDENT STAKEHOLDER REPORTING SUPPLY CHAIN COORDINATION</i>	101
P-IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	101
P-IRO-16: PUBLIC RELATIONS & REPUTATION REPAIR	102
INFORMATION ASSURANCE (IAO) PROCEDURES	103
P-IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS	103
P-IAO-02: SECURITY ASSESSMENTS	103
<i>P-IAO-02.4: SECURITY ASSESSMENTS SECURITY ASSESSMENT REPORT (SAR)</i>	104
<i>P-IAO-03.2: SYSTEM SECURITY & PRIVACY PLAN (SSPP) ADEQUATE SECURITY FOR SENSITIVE / REGULATED DATA IN SUPPORT OF CONTRACTS</i>	105
P-IAO-05: PLAN OF ACTION & MILESTONES (POA&M)	106
MAINTENANCE (MNT) PROCEDURES	107
P-MNT-01: MAINTENANCE OPERATIONS	107
P-MNT-02: CONTROLLED MAINTENANCE	107
P-MNT-03: TIMELY MAINTENANCE	108
<i>P-MNT-03.1: TIMELY MAINTENANCE PREVENTATIVE MAINTENANCE</i>	108
NETWORK SECURITY (NET) PROCEDURES	110
P-NET-01: NETWORK SECURITY CONTROLS (NSC)	110
P-NET-02: LAYERED DEFENSES	110
P-NET-18: DNS & CONTENT FILTERING	111
PHYSICAL & ENVIRONMENTAL SECURITY (PES) PROCEDURE	112
P-PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS	112
P-PES-02: PHYSICAL ACCESS AUTHORIZATIONS	112
<i>P-PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS ROLE-BASED PHYSICAL ACCESS</i>	113
P-PES-03: PHYSICAL ACCESS CONTROL	113
<i>P-PES-03.3: PHYSICAL ACCESS CONTROL PHYSICAL ACCESS LOGS</i>	115
P-PES-05: MONITORING PHYSICAL ACCESS	115
P-PES-07: SUPPORTING UTILITIES	116
<i>P-PES-07.5: SUPPORTING UTILITIES WATER DAMAGE PROTECTION</i>	116
P-PES-08: FIRE PROTECTION	117
P-PES-09: TEMPERATURE & HUMIDITY CONTROLS	117
DATA PRIVACY (PRI) PROCEDURES	118
P-PRI-01: DATA PRIVACY PROGRAM	118
P-PRI-05: PERSONAL DATA RETENTION & DISPOSAL	118
<i>P-PRI-05.5: PERSONAL DATA RETENTION & DISPOSAL INVENTORY OF PERSONAL DATA</i>	119
P-PRI-07: INFORMATION SHARING WITH THIRD PARTIES	119
<i>P-PRI-07.1: INFORMATION SHARING WITH THIRD PARTIES PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS</i>	120
PROJECT & RESOURCE MANAGEMENT (PRM) PROCEDURES	121
P-PRM-01: CYBERSECURITY & DATA PRIVACY PORTFOLIO MANAGEMENT	121
<i>P-PRM-01.1: CYBERSECURITY & DATA PRIVACY PORTFOLIO MANAGEMENT STRATEGIC PLAN & OBJECTIVES</i>	121
P-PRM-02: CYBERSECURITY & DATA PRIVACY RESOURCE MANAGEMENT	122
P-PRM-03: ALLOCATION OF RESOURCES	122
P-PRM-07: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT	123
RISK MANAGEMENT (RSK) PROCEDURES	124
P-RSK-01: RISK MANAGEMENT PROGRAM (RMP)	124
<i>P-RSK-01.1: RISK MANAGEMENT PROGRAM (RMP) RISK FRAMING</i>	124
<i>P-RSK-01.3: RISK MANAGEMENT PROGRAM (RMP) RISK TOLERANCE</i>	125
<i>P-RSK-01.4: RISK MANAGEMENT PROGRAM (RMP) RISK THRESHOLD</i>	125
<i>P-RSK-01.5: RISK MANAGEMENT PROGRAM (RMP) RISK APPETITE</i>	126
P-RSK-02: RISK-BASED SECURITY CATEGORIZATION	126
<i>P-RSK-02.1: RISK-BASED SECURITY CATEGORIZATION IMPACT-LEVEL PRIORITIZATION</i>	127
P-RSK-03: RISK IDENTIFICATION	127
<i>P-RSK-03.1: RISK IDENTIFICATION RISK CATALOG</i>	127
P-RSK-04: RISK ASSESSMENT	128
<i>P-RSK-04.1: RISK ASSESSMENT RISK REGISTER</i>	129
P-RSK-05: RISK RANKING	129
P-RSK-06: RISK REMEDIATION	130

P-RSK-06.1: RISK REMEDIATION RISK RESPONSE	130
P-RSK-06.2: RISK REMEDIATION COMPENSATING COUNTERMEASURES	131
P-RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM	131
P-RSK-09.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM SUPPLY CHAIN RISK ASSESSMENT	132
P-RSK-12: RISK CULTURE	133
SECURE ENGINEERING & ARCHITECTURE (SEA) PROCEDURE	134
P-SEA-01: SECURE ENGINEERING PRINCIPLES	134
P-SEA-01.1: SECURE ENGINEERING PRINCIPLES CENTRALIZED MANAGEMENT OF CYBERSECURITY & DATA PRIVACY CONTROLS	135
P-SEA-01.2: SECURE ENGINEERING PRINCIPLES ACHIEVING RESILIENCE REQUIREMENTS	135
P-SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE	136
P-SEA-07: PREDICTABLE FAILURE ANALYSIS	137
P-SEA-07.1: PREDICTABLE FAILURE ANALYSIS TECHNOLOGY LIFECYCLE MANAGEMENT	137
SECURITY OPERATIONS (OPS) PROCEDURES	139
P-OPS-01: OPERATIONS SECURITY	139
P-OPS-01.1: OPERATIONS SECURITY STANDARDIZED OPERATING PROCEDURES (SOP)	139
SECURITY AWARENESS & TRAINING (SAT) PROCEDURES	141
P-SAT-01: CYBERSECURITY & DATA PRIVACY-MINDED WORKFORCE	141
P-SAT-02: CYBERSECURITY & DATA PRIVACY AWARENESS TRAINING	141
P-SAT-03: CYBERSECURITY & DATA PRIVACY ROLE-BASED TRAINING	143
P-SAT-03.5: CYBERSECURITY & DATA PRIVACY TRAINING PRIVILEGED USERS	144
P-SAT-03.6: CYBERSECURITY & DATA PRIVACY TRAINING CYBER THREAT ENVIRONMENT	144
P-SAT-03.7: CYBERSECURITY & DATA PRIVACY TRAINING CONTINUING PROFESSIONAL EDUCATION (CPE) - CYBERSECURITY & DATA PRIVACY PERSONNEL	145
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) PROCEDURES	146
P-TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION	146
P-TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION PRODUCT MANAGEMENT	146
P-TDA-01.2: TECHNOLOGY DEVELOPMENT & ACQUISITION INTEGRITY MECHANISMS FOR SOFTWARE/FIRMWARE UPDATES	147
P-TDA-04: DOCUMENTATION REQUIREMENTS	147
P-TDA-04.2: DOCUMENTATION REQUIREMENTS SOFTWARE BILL OF MATERIALS (SBOM)	148
P-TDA-06: SECURE CODING	148
P-TDA-06.1: SECURE CODING CRITICALITY ANALYSIS	150
P-TDA-06.2: SECURE CODING THREAT MODELING	150
P-TDA-06.3: SECURE CODING SOFTWARE ASSURANCE MATURITY MODEL (SAMM)	151
P-TDA-09: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT	151
P-TDA-09.1: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT CONTINUOUS MONITORING PLAN	152
P-TDA-14: DEVELOPER CONFIGURATION MANAGEMENT	152
P-TDA-14.1: DEVELOPER CONFIGURATION MANAGEMENT SOFTWARE/FIRMWARE INTEGRITY VERIFICATION	153
P-TDA-14.2: DEVELOPER CONFIGURATION MANAGEMENT HARDWARE INTEGRITY VERIFICATION	153
P-TDA-17: UNSUPPORTED SYSTEMS	154
THIRD-PARTY MANAGEMENT (TPM) PROCEDURES	155
P-TPM-01: THIRD-PARTY MANAGEMENT	155
P-TPM-01.1: THIRD-PARTY MANAGEMENT THIRD-PARTY INVENTORIES	155
P-TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS	156
P-TPM-03: SUPPLY CHAIN PROTECTION	156
P-TPM-03.2: SUPPLY CHAIN PROTECTION LIMIT POTENTIAL HARM	156
P-TPM-03.3: SUPPLY CHAIN PROTECTION PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	157
P-TPM-04: THIRD-PARTY SERVICES	157
P-TPM-04.1: THIRD-PARTY SERVICES THIRD-PARTY RISK ASSESSMENTS & APPROVALS	158
P-TPM-04.3: THIRD-PARTY SERVICES CONFLICT OF INTERESTS	158
P-TPM-04.4: THIRD-PARTY SERVICES THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS	159
P-TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	159
P-TPM-05.2: THIRD-PARTY CONTRACT REQUIREMENTS CONTRACT FLOW-DOWN REQUIREMENTS	160
P-TPM-05.3: THIRD-PARTY CONTRACT REQUIREMENTS THIRD-PARTY AUTHENTICATION PRACTICES	160
P-TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX	161
P-TPM-05.5: THIRD-PARTY CONTRACT REQUIREMENTS THIRD-PARTY SCOPE REVIEW	161

<i>P-TPM-05.6: THIRD-PARTY CONTRACT REQUIREMENTS FIRST-PARTY DECLARATION (1PD)</i>	162
<i>P-TPM-05.7: THIRD-PARTY CONTRACT REQUIREMENTS BREAK CLAUSES</i>	162
P-TPM-06: THIRD-PARTY PERSONNEL SECURITY	162
P-TPM-08: REVIEW OF THIRD-PARTY SERVICES	163
P-TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION	164
P-TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES	164
P-TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	164
THREAT MANAGEMENT (THR) PROCEDURES	166
P-THR-01: THREAT AWARENESS PROGRAM	166
P-THR-02: INDICATORS OF EXPOSURE (IOE)	166
P-THR-03: THREAT INTELLIGENCE FEEDS	167
P-THR-04: INSIDER THREAT PROGRAM	167
P-THR-05: INSIDER THREAT AWARENESS	168
P-THR-07: THREAT HUNTING	169
P-THR-09: THREAT CATALOG	169
P-THR-10: THREAT ANALYSIS	169
VULNERABILITY & PATCH MANAGEMENT (VPM) PROCEDURES	171
P-VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	171
<i>P-VPM-01.1: VULNERABILITY & PATCH MANAGEMENT PROGRAM ATTACK SURFACE SCOPE</i>	171
P-VPM-02: VULNERABILITY REMEDIATION PROCESS	172
P-VPM-03: VULNERABILITY RANKING	172
P-VPM-05: SOFTWARE & FIRMWARE PATCHING	173
P-VPM-06: VULNERABILITY SCANNING	174
GLOSSARY: ACRONYMS & DEFINITIONS	176
ACRONYMS	176
DEFINITIONS	177
RECORD OF CHANGES	178

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 90% of the content as part of the template that would leave the remaining 10% 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 cybersecurity program, since procedures represents the specific activities that are performed to protect systems and data.

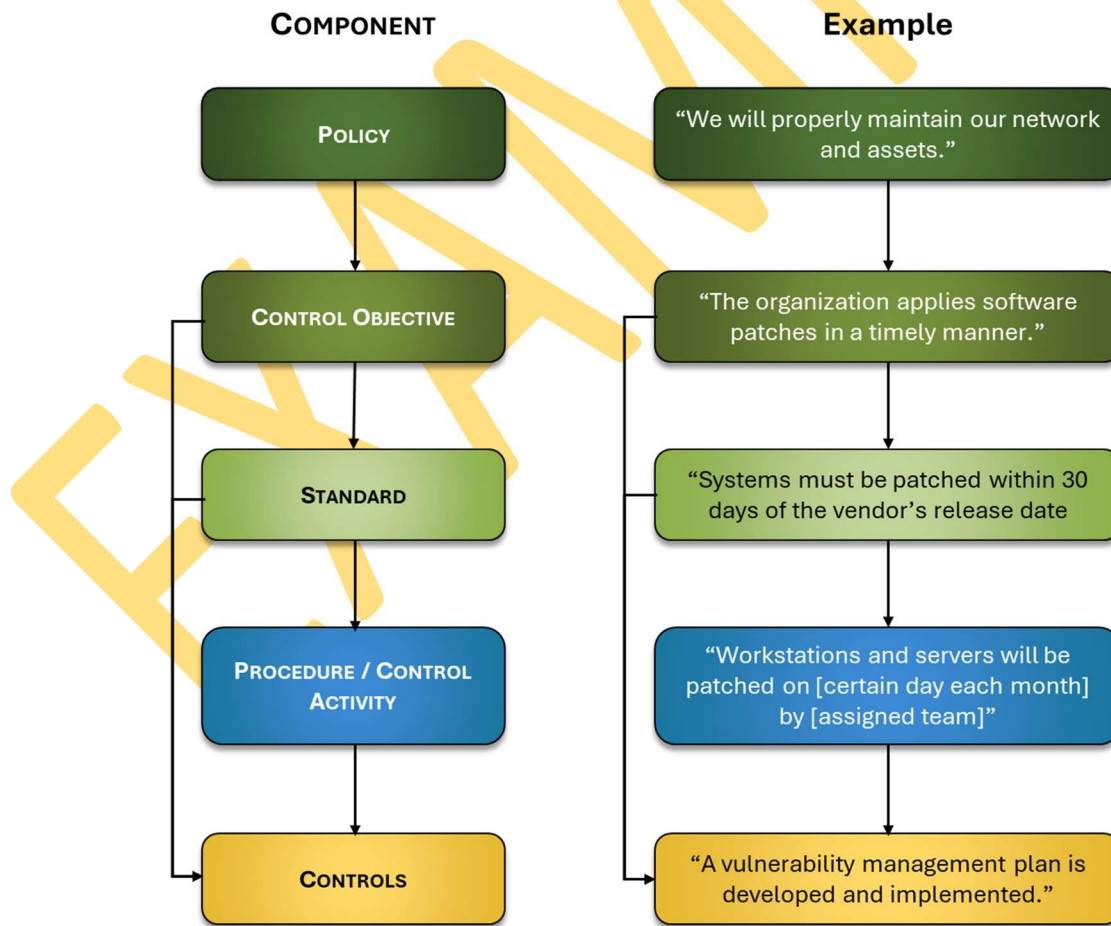
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

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

- Certain standards require processes to exist (*due diligence – 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 care – 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.



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 & data 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 v1.0.0 Cybersecurity Workforce Framework – Work Categories

EXAMPLE

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

NOTE: THIS PROCESS SECTION CAN BE USED AS A GUIDE TO TAILOR PROCEDURES

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/it/applied-cybersecurity/nice>

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 #P-CFG-02. The SCF is a free resource that can be downloaded from <https://www.securecontrolsframework.com>]*

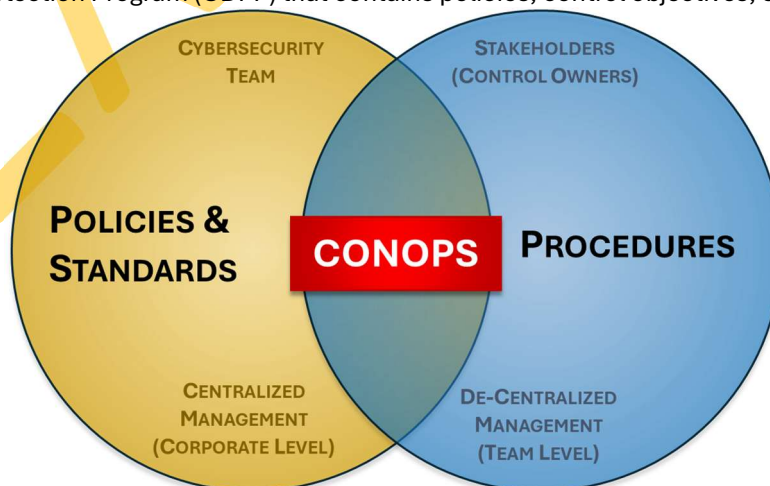
Procedure / Control Activity: Secure Systems Development [DD-WRL-004], in conjunction with the Technical Support [IO-WRL-007] and Cybersecurity Architecture [DD-WRL-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices to ensure baseline system hardening configurations for all ACME-owned or managed assets comply with applicable legal, statutory and regulatory compliance obligations throughout the System Development Life Cycle (SDLC).
- (2) Includes hardware, software, firmware and documentation in baseline configurations. 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) Technology platforms that include, but are not limited to:
 - a. Server-Class Systems
 - i. Microsoft Server 2003
 - ii. Microsoft Server 2008
 - iii. Microsoft Server 2012
 - iv. Microsoft Server 2016
 - v. Microsoft Server 2018
 - vi. Microsoft Server 2020
 - vii. Microsoft Server 2022
 - viii. Red Hat Enterprise Linux (RHEL)
 - ix. Unix
 - x. Solaris
 - b. Workstation-Class Systems
 - i. Microsoft XP
 - ii. Microsoft 7
 - iii. Microsoft 8
 - iv. Microsoft 10
 - v. Microsoft 11
 - vi. Apple
 - vii. Fedora (Linux)
 - viii. Ubuntu (Linux)
 - ix. SuSe (Linux)
 - c. Network Devices
 - i. Firewalls
 - ii. Routers
 - iii. Load balancers
 - iv. Virtual Private Network (VPN) concentrators
 - v. Wireless Access Points (WAPs)
 - vi. Wireless controllers
 - vii. Printers
 - viii. Multi-Function Devices (MFDs)
 - d. Mobile Devices
 - i. Tablets
 - ii. Mobile phones
 - iii. Other portable electronic devices
 - e. Databases
 - i. MySQL
 - ii. Windows SQL Server
 - iii. Windows SQL Express
 - iv. Oracle
 - v. DB2
- (4) Ensures that system hardening includes, but is not limited to:

- a. 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.
 - b. Configuring and documenting only the necessary ports, protocols and services to meet business needs;
 - c. 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;
 - d. 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
 - e. 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).
- (5) Documents and validates security parameters are configured to prevent misuse.
 - (6) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning or use.
 - (7) 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.
 - (8) 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.
 - (9) If necessary, requests corrective action to address identified deficiencies.
 - (10) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
 - (11) If necessary, documents the results of corrective action and notes findings.
 - (12) 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 Cybersecurity And Data Protection Program (CDPP) that contains policies, control objectives, standards and guidelines.



POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

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

- (1) Policy that establishes management's intent;
- (2) Control Objective that identifies leading practices (linked to controls);
- (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 & DATA PROTECTION GOVERNANCE (GOV) PROCEDURES

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

P-GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

Control: Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.

Procedure / Control Activity: Systems Security Management [OG-WRL-014], in conjunction with Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Develops an organization-wide cybersecurity & data privacy governance program to provide complete coverage for all cybersecurity & data 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 cybersecurity & data privacy governance program in a single document, the Cybersecurity And Data Protection Program (CDPP).
- (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: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STEERING COMMITTEE & PROGRAM OVERSIGHT

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

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Develops a steering committee to coordinate cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives.
- (2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, data 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 & data 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 & data 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: CYBERSECURITY & DATA PROTECTION 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 & data protection program.

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Develops a steering committee to coordinate cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives.
- (2) Defines the composition of the steering committee (e.g., identifies key cybersecurity, data 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 & data 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 & data privacy-related projects/initiatives accordingly:
 - a. Each project must be assigned a sponsor, typically from the submitting department;

COMPLIANCE (CPL) PROCEDURES

Management Intent: The purpose of the Compliance (CPL) procedures / control activities is to ensure safeguards are in place to be aware of and comply with applicable statutory, regulatory and contractual compliance obligations.

P-CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE

Control: Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.

Procedure / Control Activity: Compliance Manager [OG-ORG-005] In conjunction with Governance Manager [OG-ORG-001], Risk Manager [OG-ORG-003], Privacy Compliance [OG-WRL-008], Systems Security Management [OG-WRL-014], Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Implements appropriate administrative means to document the geographic location of all ACME facilities.
- (2) Utilizes the following online resources to identify changes in statutory and/or regulatory data protection requirements that impact all geographical locations:
 - a. US States - <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx>
 - b. US Federal - <https://content.next.westlaw.com/Browse/Home/PracticalLaw>
 - c. International - <https://www.dlapiperdataprotection.com>
- (3) Consults with stakeholders in Legal to determine if there are any new contractual obligation changes.
- (4) Documents any changes to statutory, regulatory and contractual compliance obligations.
- (5) Assembles key stakeholders to perform a review of ACME's policies and standards to address necessary changes, if necessary.
- (6) Incorporates feedback into an updated version of ACME's policies and standards.
- (7) By the end of the [1st, 2nd, 3rd, 4th] quarter of the calendar year, oversees the change management process to release the changes from draft to production.
- (8) 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.
- (9) If necessary, requests corrective action to address identified deficiencies.
- (10) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (11) If necessary, documents the results of corrective action and notes findings.
- (12) If necessary, requests additional corrective action to address unremediated deficiencies.

P-CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE | COMPLIANCE SCOPE

Control: Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.

Procedure / Control Activity: Compliance Manager [OG-ORG-005] In conjunction with Governance Manager [OG-ORG-001], Risk Manager [OG-ORG-003], Privacy Compliance [OG-WRL-008], Systems Security Management [OG-WRL-014], Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Implements appropriate administrative means to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations by:
 - a. Conducting an annual review of applicable statutory, regulatory and/or contractual compliance obligations;
 - b. Determining the Minimum Compliance Controls (MCR) necessary to address compliance obligations;
 - c. Determining the systems, applications, services and third-parties that are applicable to the identified controls;
 - d. Documenting the scope of statutory, regulatory and/or contractual compliance obligations;
 - e. Identifying the stakeholders who are responsible for "control ownership"; and
 - f. Sharing updated compliance scoping documentation with affected stakeholders so that all parties involved are in agreement on the scope of compliance efforts.
- (2) 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-CPL-02: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT

Control: Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.

Procedure / Control Activity: Systems Security Management [OG-WRL-014], in conjunction with Cybersecurity Architecture [DD-WRL-001] and Executive Cybersecurity Leadership [OG-WRL-007]:

- (1) Develops a continuous monitoring strategy that includes effectiveness, compliance and change monitoring:³⁰
 - a. Establishing the system-level metrics to be monitored;
 - b. Establishing organization-defined frequencies for monitoring and for assessing control effectiveness;
 - c. Ongoing control assessments in accordance with the continuous monitoring strategy;
 - d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
 - e. Correlation and analysis of information generated by control assessments and monitoring;
 - f. Response actions to address results of the analysis of control assessment and monitoring information; and
 - g. Reporting the cybersecurity & data privacy status of the system to organization-defined personnel or roles per organization-defined frequency.
- (2) Implements appropriate administrative means to ensure controls are sufficient for capturing, protecting and reviewing logs from all system components in accordance with ACME requirements to centrally manage and identify anomalies or suspicious activity to ensure the continued effectiveness of cybersecurity & data privacy controls. This includes:
 - a. Reviewing the following, at least daily:
 - i. All security events;
 - ii. Logs of all system components that store, process or transmit sensitive/regulated data or that could impact the security of sensitive/regulated data;
 - iii. Logs of all critical system components; and
 - iv. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
 - 1. Firewalls;
 - 2. Intrusion Detection Systems (IDS);
 - 3. Intrusion Prevention Systems (IPS);
 - 4. Authentication servers (e.g., Active Directory domain controllers); and
 - 5. E-commerce redirection servers.
 - b. Reviewing logs of all other system components periodically based on ACME's policies and risk management strategy, as determined by ACME's annual risk assessment; and
 - c. Following up exceptions and anomalies identified during the review process.
- (3) Develops processes for the timely detection and reporting of failures of security controls on critical systems or systems containing sensitive/regulated data, including but not limited to failure of:
 - a. Firewalls;
 - b. IDS/IPS;
 - c. FIM;
 - d. Antimalware;
 - e. Physical access controls;
 - f. Logical access controls;
 - g. Audit logging mechanisms; and
 - h. Segmentation controls (if used); and
- (4) Develops processes to respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls include:

³⁰ NIST SP 800-171A / CMMC 3.12.3 / CA.L2-3.12.3[a]