STANDARDIZED OPERATING PROCEDURES (SOP)

ACME Business Consulting, Inc.
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) PROCEDURES

P-BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)
- P-BCD-01(a): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) | COORDINATE WITH RELATED PLANS
- P-BCD-01(b): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) | COORDINATE WITH EXTERNAL SERVICE PROVIDERS
- P-BCD-01(c): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) | TRANSFER TO ALTERNATE PROCESSING / STORAGE SITE
- P-BCD-01(d): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) | RECOVERY TIME / POINT OBJECTIVES

P-BCD-02: IDENTIFY CRITICAL ASSETS
- P-BCD-02(a): IDENTIFY CRITICAL ASSETS | RESUME ALL MISSIONS & BUSINESS FUNCTIONS
- P-BCD-02(b): IDENTIFY CRITICAL ASSETS | CONTINUE ESSENTIAL MISSION & BUSINESS FUNCTIONS
- P-BCD-02(c): IDENTIFY CRITICAL ASSETS | RESUME ESSENTIAL MISSION & BUSINESS FUNCTIONS

P-BCD-03: CONTINGENCY TRAINING
- P-BCD-03(a): CONTINGENCY TRAINING | SIMULATED EVENTS
- P-BCD-03(b): CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS

P-BCD-04: CONTINGENCY PLAN TESTING & EXERCISES
- P-BCD-04(a): CONTINGENCY PLAN TESTING | COORDINATED TESTING WITH RELATED PLANS
- P-BCD-04(b): CONTINGENCY PLAN TESTING & EXERCISES | ALTERNATE STORAGE & PROCESSING SITES

P-BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED

P-BCD-06: CONTINGENCY PLANNING & UPDATES

P-BCD-07: ALTERNATIVE SECURITY MEASURES

P-BCD-08: ALTERNATE STORAGE SITE
- P-BCD-08(a): ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE
- P-BCD-08(b): ALTERNATE STORAGE SITE | ACCESSIBILITY

P-BCD-09: ALTERNATE PROCESSING SITE
- P-BCD-09(a): ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE
- P-BCD-09(b): ALTERNATE PROCESSING SITE | ACCESSIBILITY
- P-BCD-09(c): ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE
- P-BCD-09(d): ALTERNATE PROCESSING SITE | PREPARATION FOR USE
- P-BCD-09(e): ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

P-BCD-10: TELECOMMUNICATIONS SERVICES AVAILABILITY
- P-BCD-10(a): TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS
- P-BCD-10(b): TELECOMMUNICATIONS SERVICES AVAILABILITY | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS
- P-BCD-10(c): TELECOMMUNICATIONS SERVICES AVAILABILITY | PROVIDER CONTINGENCY PLAN

P-BCD-11: DATA BACKUPS
- P-BCD-11(a): DATA BACKUPS | TESTING FOR RELIABILITY & INTEGRITY
- P-BCD-11(b): DATA BACKUPS | SEPARATE STORAGE FOR CRITICAL INFORMATION
- P-BCD-11(c): DATA BACKUPS | INFORMATION SYSTEM IMAGING
- P-BCD-11(d): DATA BACKUPS | CRYPTOGRAPHIC PROTECTION
- P-BCD-11(e): DATA BACKUPS | TEST RESTORATION USING SAMPLING
- P-BCD-11(f): DATA BACKUPS | TRANSFER TO ALTERNATE STORAGE SITE
- P-BCD-11(g): DATA BACKUPS | REDUNDANT SECONDARY SYSTEM
- P-BCD-11(h): DATA BACKUPS | DUAL AUTHORIZATION

P-BCD-12: INFORMATION SYSTEM RECOVERY & RECONSTITUTION
- P-BCD-12(a): INFORMATION SYSTEM RECOVERY & RECONSTITUTION | TRANSACTION RECOVERY
- P-BCD-12(b): INFORMATION SYSTEM RECOVERY & RECONSTITUTION | FAILOVER CAPABILITY
- P-BCD-12(c): INFORMATION SYSTEM RECOVERY & RECONSTITUTION | ELECTRONIC DISCOVERY (eDiscovery)
- P-BCD-12(d): INFORMATION SYSTEM RECOVERY & RECONSTITUTION | RESTORE WITHIN TIME PERIOD

P-BCD-13: BACKUP & RESTORATION HARDWARE PROTECTION

CAPACITY & PERFORMANCE PLANNING (CAP) PROCEDURES

P-CAP-01: CAPACITY & PERFORMANCE MANAGEMENT

P-CAP-02: RESOURCE PRIORITY

P-CAP-03: CAPACITY PLANNING

CHANGE MANAGEMENT (CHG) PROCEDURES

P-CHG-01: CHANGE MANAGEMENT PROGRAM

P-CHG-02: CONFIGURATION CHANGE CONTROL
P-CHG-02(a): Configuration Change Control | Prohibition of Changes
P-CHG-02(b): Configuration Change Control | Test, Validate & Document Changes
P-CHG-02(c): Configuration Change Control | Security Representative for Change
P-CHG-02(o): Configuration Change Control | Automated Security Response
P-CHG-02(e): Configuration Change Control | Cryptographic Management

P-CHG-03: Security Impact Analysis for Changes

P-CHG-04: Access Restriction for Change
P-CHG-04(a): Access Restrictions for Change | Automated Access Enforcement / Auditing
P-CHG-04(b): Access Restrictions for Change | Signed Components
P-CHG-04(c): Access Restrictions for Change | Dual Authorization for Change
P-CHG-04(o): Access Restrictions for Change | Limit Production / Operational Privileges (Incompatible Roles)
P-CHG-04(e): Access Restrictions for Change | Library Privileges

P-CHG-05: Stakeholder Notification of Changes

P-CHG-06: Security Functionality Verification
P-CHG-06(a): Security Functionality Verification | Report Verification Results

Cloud Security (Cld) Procedures

P-Cld-01: Cloud Services
P-Cld-02: Cloud Security Architecture
P-Cld-03: Security Management Subnet
P-Cld-04: Application & Program Interface (APD) Security
P-Cld-05: Virtual Machine Images
P-Cld-06: Multi-Tenant Environments
P-Cld-07: Data Handling & Portability
P-Cld-08: Standardized Virtualization Formats
P-Cld-09 Geographic Requirements for Processing, Storage and Service Locations
P-Cld-10: Sensitive Data in Public Cloud Providers
P-Cld-11: Cloud Access Point (CAP)

Compliance (Cpl) Procedures

P-Cpl-01: Statutory, Regulatory & Contractual Compliance
P-Cpl-02: Security Controls Oversight
  P-Cpl-02(a): Security Controls Oversight | Internal Audit Function
P-Cpl-03: Security Assessments
  P-Cpl-03(a): Security Assessments | Independent Assessors
  P-Cpl-03(b): Security Assessments | Functional Review of Security Controls
P-Cpl-04: Audit Activities

Configuration Management (Cfg) Procedures

P-Cfg-01: Configuration Management Program
P-Cfg-02: System Hardening Through Baseline Configurations
  P-Cfg-02(a): System Hardening Through Baseline Configurations | Reviews & Updates
  P-Cfg-02(b): System Hardening Through Baseline Configurations | Automated Central Management & Verification
  P-Cfg-02(c): System Hardening Through Baseline Configurations | Retention of Previous Configurations
  P-Cfg-02(d): System Hardening Through Baseline Configurations | Development & Test Environments
  P-Cfg-02(e): System Hardening Through Baseline Configurations | Configure Systems, Components or Devices for High-Risk Areas
  P-Cfg-02(f): System Hardening Through Baseline Configurations | Network Device Configuration File Synchronization
  P-Cfg-02(g): System Hardening Through Baseline Configurations | Approved Deviations
  P-Cfg-02(h): System Hardening Through Baseline Configurations | Respond to Unauthorized Changes
  P-Cfg-02(i): System Hardening Through Baseline Configurations | Baseline Tailoring
P-Cfg-03: Least Functionality
  P-Cfg-03(a): Least Functionality | Periodic Review
  P-Cfg-03(b): Least Functionality | Prevent Program Execution
  P-Cfg-03(c): Least Functionality | Unauthorised or Authorized Software (Blacklisting or Whitelisting)
P-Cfg-03(d): Least Functionality | Split Tunneling
P-Cfg-04: Software Usage Restrictions
  P-Cfg-04(a): Software Usage Restrictions | Open Source Software
CONTINUOUS MONITORING (MON) Procedures

P-MON-01: Continuous Monitoring
P-MON-01(A): Continuous Monitoring | Intrusion Detection & Prevention Systems (IDS & IPS)
P-MON-01(B): Continuous Monitoring | Automated Tools for Real-Time Analysis
P-MON-01(C): Continuous Monitoring | Inbound & Outbound Communications Traffic
P-MON-01(D): Continuous Monitoring | System Generated Alerts
P-MON-01(E): Continuous Monitoring | Wireless Intrusion Detection System (WIDS)
P-MON-01(F): Continuous Monitoring | Host-Based Devices
P-MON-01(G): Continuous Monitoring | File Integrity Monitoring (FIM)
P-MON-01(H): Continuous Monitoring | Reviews & Updates
P-MON-01(I): Continuous Monitoring | Proxy Logging
P-MON-01(J): Continuous Monitoring | Deactivated Account Activity
P-MON-01(K): Continuous Monitoring | Automated Response To Suspicious Events
P-MON-01(L): Continuous Monitoring | Automated Alerts
P-MON-01(M): Continuous Monitoring | Analyze Traffic / Event Patterns
P-MON-01(N): Continuous Monitoring | Individuals Posing Greater Risk
P-MON-01(O): Continuous Monitoring | Privileged User Oversight
P-MON-01(P): Continuous Monitoring | Analyze & Prioritize Monitoring Requirements

P-MON-02: Centralized Event Log Collection
P-MON-02(A): Centralized Security Event Log Collection | Correlate Monitoring Information
P-MON-02(B): Centralized Security Event Log Collection | Central Review & Analysis
P-MON-02(C): Centralized Security Event Log Collection | Integration of Scanning & Other Monitoring Information
P-MON-02(D): Centralized Security Event Log Collection | Correlation with Physical Monitoring
P-MON-02(E): Centralized Security Event Log Collection | Permitted Actions
P-MON-02(F): Centralized Security Event Log Collection | Audit Level Adjustment
P-MON-02(G): Centralized Security Event Log Collection | System-Wide / Time-Correlated Audit Trail
P-MON-02(H): Centralized Security Event Log Collection | Changes by Authorized Individuals

P-MON-03: Content of Audit Records
P-MON-03(A): Content of Audit Records | Sensitive Audit Information
P-MON-03(B): Content of Audit Records | Audit Trails
P-MON-03(C): Content of Audit Records | Privileged Functions Logging
P-MON-03(D): Content of Audit Records | Verbosity Logging for Boundary Devices
P-MON-03(E): Content of Audit Records | Limit Personal Data (PD) in Audit Records
P-MON-03(F): Content of Audit Records | Centralized Management of Planned Audit Record Content

P-MON-04: Audit Storage Capacity

P-MON-05: Response to Audit Processing Failures
P-MON-05(A): Response to Audit Processing Failures | Real-Time Alerts
P-MON-05(B): Response to Audit Processing Failures | Audit Storage Capacity Alerting

P-MON-06: Monitoring Reporting
P-MON-06(A): Monitoring Reporting | Query Parameter Audits of Personal Data (PD)
P-MON-06(B): Monitoring Reporting | Trend Analysis Reporting

P-MON-07: Time Stamps
P-MON-07(A): Time Stamps | Synchronization with Authoritative Time Source

P-MON-08: Protection of Audit Information
P-MON-08(A): Protection of Audit Information | Audit Backup on Separate Physical Systems / Components
P-MON-08(B): Protection of Audit Information | Access by Subset of Privileged Users
P-MON-08(C): Protection of Audit Information | Cryptographic Protection of Audit Information
P-MON-08(D): Protection of Audit Information | Dual Authorization

P-MON-09: Non-Repudiation

P-MON-10: Audit Record Retention

P-MON-11: Monitoring for Information Disclosure
P-MON-11(A): Monitoring for Information Disclosure | Analyze Traffic for Covert Exfiltration
P-MON-11(B): Monitoring for Information Disclosure | Unauthorized Network Services
CRYPTOGRAPHIC PROTECTIONS (CRY) Procedures

P-CRY-01: USE OF CRYPTOGRAPHIC CONTROLS
- P-CRY-01(a): USE OF CRYPTOGRAPHIC CONTROLS | ALTERNATE PHYSICAL PROTECTION
- P-CRY-01(b): USE OF CRYPTOGRAPHIC CONTROLS | EXPORT-CONTROLLED TECHNOLOGY
- P-CRY-01(c): USE OF CRYPTOGRAPHIC CONTROLS | PRE/POST TRANSMISSION HANDLING
- P-CRY-01(d): USE OF CRYPTOGRAPHIC CONTROLS | CONCEAL/RANDOMIZE COMMUNICATIONS

P-CRY-02: CRYPTOGRAPHIC MODULE AUTHENTICATION

P-CRY-03: TRANSMISSION CONFIDENTIALITY

P-CRY-04: TRANSMISSION INTEGRITY

P-CRY-05: ENCRYPTING DATA AT REST
- P-CRY-05(a): ENCRYPTING DATA AT REST | STORAGE MEDIA
- P-CRY-05(b): ENCRYPTING DATA AT REST | OFFLINE STORAGE

P-CRY-06: NON-CONSOLE ADMINISTRATIVE ACCESS

P-CRY-07: WIRELESS ACCESS AUTHENTICATION & ENCRYPTION

P-CRY-08: PUBLIC KEY INFRASTRUCTURE (PKI)
- P-CRY-08(a): PUBLIC KEY INFRASTRUCTURE (PKI) | AVAILABILITY

P-CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT
- P-CRY-09(a): CRYPTOGRAPHIC KEY MANAGEMENT | SYMMETRIC KEYS
- P-CRY-09(b): CRYPTOGRAPHIC KEY MANAGEMENT | ASYMMETRIC KEYS
- P-CRY-09(c): CRYPTOGRAPHIC KEY MANAGEMENT | CRYPTOGRAPHIC KEY LOSS OR CHANGE
- P-CRY-09(d): CRYPTOGRAPHIC KEY MANAGEMENT | CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS
- P-CRY-09(e): CRYPTOGRAPHIC KEY MANAGEMENT | ASSIGNED OWNERS

P-CRY-10: TRANSMISSION OF SECURITY & PRIVACY ATTRIBUTES

DATA CLASSIFICATION & HANDLING (DCH) Procedures

P-DCH-01: DATA PROTECTION
- P-DCH-01(a): DATA PROTECTION | DATA STEWARDSHIP

P-DCH-02: DATA & ASSET CLASSIFICATION

P-DCH-03: MEDIA ACCESS
- P-DCH-03(a): MEDIA ACCESS | DISCLOSURE OF INFORMATION
- P-DCH-03(b): MEDIA ACCESS | MASKING DISPLAYED DATA

P-DCH-04: MEDIA MARKING
- P-DCH-04(a): MEDIA MARKING | AUTOMATED MARKING

P-DCH-05: SECURITY ATTRIBUTES
- P-DCH-05(a): SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION
- P-DCH-05(b): SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS
- P-DCH-05(c): SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM
- P-DCH-05(d): SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS
- P-DCH-05(e): SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES
- P-DCH-05(f): SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION
- P-DCH-05(g): SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION
- P-DCH-05(h): SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES & TECHNOLOGIES
- P-DCH-05(i): SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT
- P-DCH-05(j): SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS
- P-DCH-05(k): SECURITY ATTRIBUTES | AUDIT CHANGES

P-DCH-06: MEDIA STORAGE
- P-DCH-06(a): MEDIA STORAGE | PHYSICALLY SECURE ALL MEDIA
- P-DCH-06(b): MEDIA STORAGE | SENSITIVE DATA INVENTORIES
P-DCH-06(c): Media Storage | Periodic Scans for Sensitive Data 189
P-DCH-06(d): Media Storage | Making Sensitive Data Unreadable In Storage 189
P-DCH-06(e): Media Storage | Storing Authentication Data 190

P-DCH-07: Media Transportation 191
P-DCH-07(a): Media Transportation | Custodians 192
P-DCH-07(b): Media Transportation | Encrypting Data In Storage Media 192

P-DCH-08: Physical Media Disposal 193
P-DCH-09: Digital Media Sanitization 194
P-DCH-09(a): Media Sanitization | Media Sanitization Documentation 194
P-DCH-09(b): Media Sanitization | Equipment Testing 195
P-DCH-09(c): Media Sanitization | Destruction of Personal Data (PD) 195
P-DCH-09(d): Media Sanitization | Non-Destructive Techniques 196
P-DCH-09(e): Media Sanitization | Dual Authorization 196

P-DCH-10: Media Use 197
P-DCH-10(a): Media Use | Limitations on Use 197
P-DCH-10(b): Media Use | Prohibit Use Without Owner 198

P-DCH-11: Media Downinggrading 199

P-DCH-12: Removable Media Security 200

P-DCH-13: Use of External Information Systems 200
P-DCH-13(a): Use of External Information Systems | Limits of Authorized Use 200
P-DCH-13(b): Use of External Information Systems | Portable Storage Devices 201
P-DCH-13(c): Use of External Information Systems | Protecting Sensitive Information on External Systems 202
P-DCH-13(d): Use of External Information Systems | Non-Organizationally Owned Systems / Components / Devices 203

P-DCH-14: Information Sharing 204
P-DCH-14(a): Information Sharing | Information Search & Retrieval 204

P-DCH-15: Publicly Accessible Content 205

P-DCH-16: Data Mining Protection 205

P-DCH-17: Ad-Hoc Transfers 206

P-DCH-18: Media & Data Retention 207
P-DCH-18(a): Media & Data Retention | Limit Personal Data (PD) Elements In Testing, Training & Research 208
P-DCH-18(b): Media & Data Retention | Minimize Personal Data (PD) 209
P-DCH-18(c): Media & Data Retention | Temporary Files Containing Personal Data 209

P-DCH-19: Geographic Location of Data 210

P-DCH-20: Archived Data Sets 210

P-DCH-21: Information Disposal 211

P-DCH-22: Data Quality Operations 212
P-DCH-22(a): Data Quality Operations | Updating & Correcting Personal Data (PD) 213
P-DCH-22(b): Data Quality Operations | Data Tags 213
P-DCH-22(c): Data Quality Operations | Personal Data (PD) Collection 214

P-DCH-23: De-Identification 215
P-DCH-23(a): De-Identification | Collection 215
P-DCH-23(b): De-Identification | Archiving 216
P-DCH-23(c): De-Identification | Release 216
P-DCH-23(d): De-Identification | Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers 217
P-DCH-23(e): De-Identification | Statistical Disclosure Control 218
P-DCH-23(f): De-Identification | Differential Privacy 218
P-DCH-23(g): De-Identification | Validated Software 219
P-DCH-23(h): De-Identification | Motivated Intruder 220

P-DCH-24: Information Location 220
P-DCH-24(a): Information Location | Automated Tools to Support Information Location 221

P-DCH-25: Transfer of Personal Information 222

Embedded Technology (EMB) Procedures 223
P-EMB-01: Embedded Technology Security Program 223
P-EMB-02: Internet of Things (IoT) 224
P-EMB-03: Operational Technology (OT) 224

Endpoint Security (END) Procedures 226

It is prohibited to disclose this document to third-parties without an executed non-disclosure agreement (NDA)
IDENTIFICATION & AUTHENTICATION (IAC) Procedures 275

P-IAC-01: Identity & Access Management (IAM) 275

P-IAC-02: Identification & Authentication for Organizational Users 275

P-IAC-02(a): Identification & Authentication for Organizational Users | Group Authentication 276

P-IAC-02(b): Identification & Authentication for Organizational Users | Network Access to Privileged Accounts - Replay Resistant 277

P-IAC-02(c): Identification & Authentication for Organizational Users | Acceptance of PIV Credentials 277

P-IAC-02(d): Identification & Authentication for Organizational Users | Out-of-Band Authentication (OOBA) 278

P-IAC-03: Identification & Authentication for Non-Organizational Users 278

P-IAC-03(a): Identification & Authentication for Non-Organizational Users | Acceptance of PIV Credentials from Other Organizations 279

P-IAC-03(b): Identification & Authentication for Non-Organizational Users | Acceptance of Third-Party Credentials 280

P-IAC-03(c): Identification & Authentication for Non-Organizational Users | Use of FICAM-Issued Profiles 280

P-IAC-03(d): Identification & Authentication for Non-Organizational Users | Disassociability 281

P-IAC-04: Identification & Authentication for Devices 282

P-IAC-04(a): Identification & Authentication for Devices | Device Attestation 282

P-IAC-05: Identification & Authentication for Third Party Systems & Services 283

P-IAC-05(a): Identification & Authentication for Third Party Systems & Services | Information Exchange 283

P-IAC-06: Multi-factor Authentication (MFA) 284

P-IAC-06(a): Multi-Factor Authentication (MFA) | Network Access to Privileged Accounts 284

P-IAC-06(b): Multi-Factor Authentication (MFA) | Network Access to Non-Privileged Accounts 285

P-IAC-06(c): Multi-Factor Authentication (MFA) | Local Access to Privileged Accounts 286

P-IAC-06(d): Multi-Factor Authentication (MFA) | Out of Band (OOB) Factor 286

P-IAC-07: User Provisioning & De-Provisioning 287

P-IAC-07(a): User Provisioning & De-Provisioning | Change of Roles & Duties 287

P-IAC-07(b): User Provisioning & De-Provisioning | Termination of Employment 288

P-IAC-08: Role-Based Access Control (RBAC) 289

P-IAC-09: Identifier Management (User Names) 289

P-IAC-09(a): Identifier Management | User Identity (ID) Management 291

P-IAC-09(b): Identifier Management | Identity User Status 292

P-IAC-09(c): Identifier Management | Dynamic Management 292

P-IAC-09(d): Identifier Management | Cross-Organization Management 293

P-IAC-09(e): Identifier Management | Privileged Account Identifiers 294

P-IAC-09(f): Identifier Management | Pairwise Pseudonymous Identifiers (PPID) 295

P-IAC-10: Authenticator Management (Passwords) 296

P-IAC-10(a): Authenticator Management | Password-Based Authentication 297

P-IAC-10(b): Authenticator Management | PKI-Based Authentication 297

P-IAC-10(c): Authenticator Management | In-Person or Trusted Third-Party Registration 298

P-IAC-10(d): Authenticator Management | Automated Support For PasswordStrength 298
P-IAC-10(e): Authenticator Management | Protection of Authenticators
P-IAC-10(f): Authenticator Management | No Embedded Unencrypted Static Authenticators
P-IAC-10(g): Authenticator Management | Hardware Token-Based Authentication
P-IAC-10(h): Authenticator Management | Vendor-Supplied Defaults
P-IAC-10(i): Authenticator Management | Multiple Information System Accounts
P-IAC-10(j): Authenticator Management | Expiration of Cached Authenticators

P-IAC-11: Authenticator Feedback

P-IAC-12: Cryptographic Module Authentication

P-IAC-13: Adaptive Identification & Authentication

P-IAC-14: Re-Authentication

P-IAC-15: Account Management

P-IAC-15(a): Account Management | Automated System Account Management
P-IAC-15(b): Account Management | Removal of Temporary / Emergency Accounts
P-IAC-15(c): Account Management | Disable Inactive Accounts
P-IAC-15(d): Account Management | Automated Audit Actions
P-IAC-15(e): Account Management | Restrictions on Shared Groups / Accounts
P-IAC-15(f): Account Management | Account Disabling for High Risk Individuals
P-IAC-15(g): Account Management | System Accounts
P-IAC-15(h): Account Management | Usage Conditions

P-IAC-16: Privileged Account Management (PAM)

P-IAC-16(a): Privileged Account Management (PAM) | Privileged Account Inventories

P-IAC-17: Periodic Review

P-IAC-18: User Responsibilities for Account Management

P-IAC-19: Credential Sharing

P-IAC-20: Access Enforcement

P-IAC-20(a): Access Enforcement | Access To Sensitive Data
P-IAC-20(b): Access Enforcement | Database Access
P-IAC-20(c): Access Enforcement | Use of Privileged Utility Programs
P-IAC-20(d): Access Enforcement | Dedicated Administrative Machines
P-IAC-20(e): Access Enforcement | Dual Authorization for Privileged Commands

P-IAC-21: Least Privilege

P-IAC-21(a): Least Privilege | Authorize Access to Security Functions
P-IAC-21(b): Least Privilege | Non-Privileged Access for Non-Security Functions
P-IAC-21(c): Least Privilege | Privileged Accounts
P-IAC-21(d): Least Privilege | Auditing Use of Privileged Functions
P-IAC-21(e): Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions
P-IAC-21(f): Least Privilege | Network Access to Privileged Commands
P-IAC-21(g): Least Privilege | Privilege Levels for Code Execution

P-IAC-22: Account Lockout

P-IAC-23: Concurrent Session Control

P-IAC-24: Session Lock

P-IAC-24(a): Session Lock | Pattern-Hiding Displays

P-IAC-25: Session Termination

P-IAC-26: Permitted Actions Without Identification or Authorization

P-IAC-27: Reference Monitor

P-IAC-28: Identity Proofing

P-IAC-28(a): Identity Proofing | Supervisor Authorization
P-IAC-28(b): Identity Proofing | Identity Evidence
P-IAC-28(c): Identity Proofing | Identity Evidence Validation & Verification
P-IAC-28(d): Identity Proofing | In-Person Validation & Verification
P-IAC-28(e): Identity Proofing | Address Confirmation

Incident Response (IRO) Procedures

P-IRO-01: Incidents Response Operations

P-IRO-02: Incident Handling

P-IRO-02(a): Incident Handling | Automated Incident Handling Processes
P-IRO-02(b): Incident Handling | Identity Theft Protection Program (ITPP)
P-IRO-02(c): Incident Handling | Dynamic Reconfiguration
P-IRO-02(d): Incident Handling | Continuity of Operations

Internal Use

It is prohibited to disclose this document to third-parties without an executed non-disclosure agreement (NDA)
P-MNT-05(a): Non-Local Maintenance | Auditing 374
P-MNT-05(b): Non-Local Maintenance | Notification of Non-Local Maintenance 374
P-MNT-05(c): Non-Local Maintenance | Cryptographic Protection 375
P-MNT-05(d): Non-Local Maintenance | Remote Disconnect Verification 376
P-MNT-05(e): Non-Local Maintenance | Pre-Approval of Non-Local Maintenance 376
P-MNT-05(f): Non-Local Maintenance | Comparable Security & Sanitization 377
P-MNT-06: Maintenance Personnel 377
  P-MNT-06(a): Maintenance Personnel | Maintenance Personnel Without Appropriate Access 378
  P-MNT-06(b): Maintenance Personnel | Non-System Related Maintenance 379

**Mobile Device Management (MDM) Procedures** 380

P-MDM-01: Centralized Management Of Mobile Devices 380
P-MDM-02: Access Control For Mobile Devices 380
P-MDM-03: Full Device & Container-Based Encryption 382
P-MDM-04: Tamper Protection & Detection 382
P-MDM-05: Remote Purging 383
P-MDM-06: Personally-Owned Mobile Devices 383
P-MDM-07: Organization-Owned Mobile Devices 385
P-MDM-08: Mobile Device Data Retention Limitations 385

**Network Security (NET) Procedures** 387

P-NET-01: Network Security Management 387
P-NET-02: Layered Defenses 387
  P-NET-02(a): Layered Defenses | Denial of Service (DoS) Protection 388
  P-NET-02(b): Layered Defenses | Guest Networks 389
P-NET-03: Boundary Protection 390
  P-NET-03(a): Boundary Protection | Access Points 391
  P-NET-03(b): Boundary Protection | External Telecommunications Services 391
  P-NET-03(c): Boundary Protection | Internal Network Address Space 392
  P-NET-03(d): Boundary Protection | Personal Data (PD) 393
  P-NET-03(e): Boundary Protection | Prevent Unauthorized Exfiltration 393
  P-NET-03(f): Boundary Protection | Dynamic Isolation & Segregation (Sandboxing) 394
  P-NET-03(g): Boundary Protection | Isolation of Information System Components (DMZ) 394
  P-NET-03(h): Boundary Protection | Separate Subnets For Connecting To Different Security Domains 395
P-NET-04: Data Flow Enforcement - Access Control Lists (ACls) 395
  P-NET-04(a): Data Flow Enforcement | Deny Traffic by Default & Allow Traffic by Exception 396
  P-NET-04(b): Data Flow Enforcement | Object Security Attributes 397
  P-NET-04(c): Data Flow Enforcement | Content Check For Encrypted Data 397
  P-NET-04(d): Data Flow Enforcement | Embedded Data Types 398
  P-NET-04(e): Data Flow Enforcement | Metadata 398
  P-NET-04(f): Data Flow Enforcement | Human Reviews 399
  P-NET-04(g): Data Flow Enforcement | Security Policy Filters 400
  P-NET-04(h): Data Flow Enforcement | Data Type Identifiers 400
  P-NET-04(i): Data Flow Enforcement | Decomposition Into Policy-Relevant Subcomponents 401
  P-NET-04(j): Data Flow Enforcement | Detection of Unsanctioned Information 401
  P-NET-04(k): Data Flow Enforcement | Approved Solutions 402
P-NET-05: System Interconnections 402
  P-NET-05(a): System Interconnections | External System Connections 403
  P-NET-05(b): System Interconnections | Internal System Connections 404
P-NET-06: Network Segmentation 404
  P-NET-06(a): Security Function Isolation | Security Management Subnets 405
  P-NET-06(b): Security Function Isolation | Virtual Local Area Network (VLAN) Separation 406
P-NET-07: Network Disconnect 407
P-NET-08: Network Intrusion Detection & Prevention Systems (NIDS / NIPS) 408
  P-NET-08(a): Network Intrusion Detection & Prevention Systems (NIDS / NIPS) | DMZ Networks 408
P-NET-09: Session Authenticity 410
  P-NET-09(a): Session Authenticity | Invalidate Session Identifiers at Logout 410
P-NET-10 Domain Name Service (DNS) Resolution
  P-NET-10(a): Domain Name Service (DNS) Resolution | Architecture & Provisioning For Name / Address Resolution Service
  P-NET-10(b): Domain Name Service (DNS) Resolution | Secure Name / Address Resolution Service (Recursive or Caching Resolver)

P-NET-11: Out-of-Band Channels

P-NET-12: Safeguarding Data Over Open Networks
  P-NET-12(a): Safeguarding Date Over Open Networks | Wireless Link Protection
  P-NET-12(b): Safeguarding Date Over Open Networks | End-User Messaging Technologies

P-NET-13: Electronic Messaging

P-NET-14: Remote Access
  P-NET-14(a): Remote Access | Automated Monitoring & Control
  P-NET-14(b): Remote Access | Protection of Confidentiality / Integrity Using Encryption
  P-NET-14(c): Remote Access | Managed Access Control Points
  P-NET-14(d): Remote Access | Privileged Commands & Access
  P-NET-14(e): Remote Access | Telecommuting
  P-NET-14(g): Remote Access | Endpoint Security Validation
  P-NET-14(h): Remote Access | Expeditions Disconnect / Disable Capability

P-NET-15: Wireless Networking
  P-NET-15(a): Wireless Access | Authentication & Encryption
  P-NET-15(c): Wireless Access | Restrict Configuration By Users

P-NET-16: Intranets

P-NET-17: Data Loss Prevention (DLP)

P-NET-18: Content Filtering
  P-NET-18(a): Content Filtering | Route Traffic To Proxy Servers

Physical & Environmental Security (PES) Procedures

P-PES-01: Physical & Environmental Protections

P-PES-02: Physical Access Authorizations
  P-PES-02(a): Physical Access Authorizations | Role-Based Physical Access

P-PES-03: Physical Access Control
  P-PES-03(a): Physical Access Control | Controlled Ingress & Egress Points
  P-PES-03(b): Physical Access Control | Lockable Physical Casings
  P-PES-03(c): Physical Access Control | Physical Access Logs
  P-PES-03(d): Physical Access Control | Access To Information Systems

P-PES-04: Physical Security of Offices, Rooms & Facilities
  P-PES-04(a): Physical Security of Offices, Rooms & Facilities | Working in Secure Areas

P-PES-05: Monitoring Physical Access
  P-PES-05(a): Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment
  P-PES-05(b): Monitoring Physical Access | Monitoring Physical Access To Information Systems

P-PES-06: Visitor Control
  P-PES-06(a): Visitor Control | Distinguish Visitors from On-Site Personnel
  P-PES-06(b): Visitor Control | Identification Requirement
  P-PES-06(c): Visitor Control | Restrict Unescorted Access
  P-PES-06(d): Visitor Control | Automated Records Management & Review

P-PES-07: Supporting Utilities
  P-PES-07(a): Supporting Utilities | Automatic Voltage Controls
  P-PES-07(b): Supporting Utilities | Emergency Shutoff
  P-PES-07(c): Supporting Utilities | Emergency Power
  P-PES-07(d): Supporting Utilities | Emergency Lighting
  P-PES-07(e): Supporting Utilities | Water Damage Protection
  P-PES-07(f): Supporting Utilities | Automation Support for Water Damage Protection

P-PES-08: Fire Protection
  P-PES-08(a): Fire Protection | Fire Detection Devices
  P-PES-08(b): Fire Protection | Fire Suppression Devices
P-PRI-01: PRIVACY PROGRAM

P-PRI-02: PRIVACY NOTICE

P-PRI-03: CHOICE & CONSENT

P-PRI-04: COLLECTION

P-PRI-05: USE, RETENTION & DISPOSAL

P-PRI-06: DATA SUBJECT ACCESS

P-PRI-07: INFORMATION SHARING WITH THIRD PARTIES

P-PRI-08: TESTING, TRAINING & MONITORING

P-PRI-09: PERSONAL DATA LINEAGE

P-PRI-10: DATA QUALITY MANAGEMENT

P-PRI-11: DATA TAGGING

P-PRI-12: UPDATING PERSONAL DATA (PD)

P-PRI-13: DATA MANAGEMENT BOARD

P-PRI-14: PRIVACY REPORTING

Privacy (PRI) Procedures
PROJECT & RESOURCE MANAGEMENT (PRM) PROCEDURES

P-PRM-01: SECURITY PORTFOLIO MANAGEMENT
  P-PRM-01(a): SECURITY PORTFOLIO MANAGEMENT | STRATEGIC PLAN & OBJECTIVES
  P-PRM-01(b): SECURITY PORTFOLIO MANAGEMENT | TARGETED CAPABILITY MATURITY LEVELS

P-PRM-02: INFORMATION SECURITY RESOURCE MANAGEMENT

P-PRM-03: ALLOCATION OF RESOURCES

P-PRM-04: SECURITY & PRIVACY IN PROJECT MANAGEMENT

P-PRM-05: SECURITY & PRIVACY REQUIREMENTS DEFINITION

P-PRM-06: BUSINESS PROCESS DEFINITION

P-PRM-07: SECURE DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT

P-PRM-08: MANAGE ORGANIZATIONAL KNOWLEDGE

RISK MANAGEMENT (RSK) PROCEDURES

P-RSK-01: RISK MANAGEMENT PROGRAM
  P-RSK-01(a): RISK MANAGEMENT PROGRAM (RMP) | RISK FRAMING

P-RSK-02: RISK-BASED SECURITY CATEGORIZATION

P-RSK-03: RISK IDENTIFICATION

P-RSK-04: RISK ASSESSMENT
  P-RSK-04(a): RISK ASSESSMENT | RISK REGISTER

P-RSK-05: RISK RANKING

P-RSK-06: RISK REMEDIATION
  P-RSK-06(a): RISK REMEDIATION | RISK RESPONSE

P-RSK-07: RISK ASSESSMENT UPDATE

P-RSK-08: BUSINESS IMPACT ANALYSIS (BIA)

P-RSK-09: SUPPLY CHAIN RISK MANAGEMENT PLAN
  P-RSK-09(a): SUPPLY CHAIN RISK MANAGEMENT PLAN | SUPPLY CHAIN RISK ASSESSMENT

P-RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)

SECURE ENGINEERING & ARCHITECTURE (SEA) PROCEDURES

P-SEA-01: SECURE ENGINEERING PRINCIPLES
  P-SEA-01(a): SECURE ENGINEERING PRINCIPLES | CENTRALIZED MANAGEMENT OF CYBERSECURITY & PRIVACY CONTROLS

P-SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE
  P-SEA-02(a): ALIGNMENT WITH ENTERPRISE ARCHITECTURE | STANDARDIZED TERMINOLOGY

P-SEA-03: DEFENSE-IN-DEPTH (DID) ARCHITECTURE
  P-SEA-03(a): DEFENSE-IN-DEPTH (DID) ARCHITECTURE | SYSTEM PARTITIONING
  P-SEA-03(b): DEFENSE-IN-DEPTH (DID) ARCHITECTURE | APPLICATION PARTITIONING

P-SEA-04: PROCESS ISOLATION
  P-SEA-04(a): PROCESS ISOLATION | SECURITY FUNCTION ISOLATION
  P-SEA-04(b): PROCESS ISOLATION | HARDWARE SEPARATION
  P-SEA-04(c): PROCESS ISOLATION | THREAD SEPARATION

P-SEA-05: INFORMATION IN SHARED RESOURCES

P-SEA-06: PREVENT PROGRAM EXECUTION

P-SEA-07: PREDICTABLE FAILURE ANALYSIS
  P-SEA-07(a): PREDICTABLE FAILURE ANALYSIS | TECHNOLOGY LIFECYCLE MANAGEMENT
  P-SEA-07(b): PREDICTABLE FAILURE ANALYSIS | FAILOUT
  P-SEA-07(c): PREDICTABLE FAILURE ANALYSIS | FAILOUT-

P-SEA-08: NON-PERSISTENCE
  P-SEA-08(a): NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES

P-SEA-09: INFORMATION OUTPUT FILTERING
  P-SEA-09(a): INFORMATION OUTPUT FILTERING | LIMIT PERSONAL DATA (PD) DISSEMINATION

P-SEA-10: MEMORY PROTECTION

P-SEA-11: HONEYPOTS

P-SEA-12: HONEYCLIENTS

P-SEA-13: HETEROGENEITY
  P-SEA-13(a): HETEROGENEITY | VIRTUALIZATION TECHNIQUES

P-SEA-14: CONCEALMENT & MISDIRECTION
P-SEA-14(a): Concealment & Misdirection / Randomness 521
P-SEA-14(b): Concealment & Misdirection / Change Processing & Storage Locations 521
P-SEA-15: Distributed Processing & Storage 522
P-SEA-16: Non-Modifiable Executable Programs 522
P-SEA-17: Secure Log-On Procedures 523
P-SEA-18: System Use Notification (Logon Banner) 524
  P-SEA-18(a): System Use Notification / Standardized Microsoft Windows Banner 524
  P-SEA-18(b): System Use Notification / Truncated Banner 525
P-SEA-19: Previous Logon Notification 526
P-SEA-20: Clock Synchronization 526

Security Operations (OPS) Procedures 528
P-OPS-01: Operations Security 528
  P-OPS-01(a): Operations Security / Standardized Operating Procedures (SOP) 528
P-OPS-02: Security Concept Of Operations (CONOPS) 529
P-OPS-03: Service Delivery (Business Process Support) 530
P-OPS-04: Security Operations Center (SOC) 531

Security Awareness & Training (SAT) Procedures 532
P-SAT-01: Security & Privacy-Minded Workforce 532
P-SAT-02: Security & Privacy Awareness 532
  P-SAT-02(a): Security Awareness / Practical Exercises 533
  P-SAT-02(b): Security Awareness / Social Engineering & Mining 534
P-SAT-03: Security & Privacy Training 535
  P-SAT-03(a): Security & Privacy Training / Practical Exercises 535
  P-SAT-03(b): Security & Privacy Training / Suspicious Communications & Anomalous System Behavior 536
  P-SAT-03(c): Security & Privacy Training / Sensitive Information Storage, Handling & Processing 537
  P-SAT-03(d): Security & Privacy Training / Vendor Security Training 537
  P-SAT-03(e): Security & Privacy Training / Privileged Users 538
P-SAT-04: Security & Privacy Training Records 539

Technology Development & Acquisition (TDA) Procedures 540
P-TDA-01: Technology Development & Acquisition 540
  P-TDA-01(A): Technology Development & Acquisition / Product Management 540
  P-TDA-01(b): Technology Development & Acquisition / Integrity Mechanisms for Software / Firmware Updates 541
  P-TDA-01(c): Technology Development & Acquisition / Malware Testing Prior To Release 542
P-TDA-02: Security Requirements 543
  P-TDA-02(A): Security Requirements / Ports, Protocols & Services In Use 543
  P-TDA-02(b): Security Requirements / Use Of Approved PIV Products 544
  P-TDA-02(c): Security Requirements / Development Methods, Techniques & Processes 544
P-TDA-03: Commercial Off-The-Shelf (COTS) Security Solutions 545
  P-TDA-03(A): Commercial Off-The-Shelf (COTS) Security Solutions / Supplier Diversity 545
P-TDA-04: Documentation Requirements 546
  P-TDA-04(A): Documentation Requirements / Functional Properties 547
P-TDA-05: Developer Architecture & Design 548
P-TDA-06: Secure Coding 549
  P-TDA-06(A): Secure Coding / Criticality Analysis 550
P-TDA-07: Secure Development Environments 550
P-TDA-08: Separation of Development, Testing & Operational Environments 551
P-TDA-09: Security & Privacy Testing Throughout Development 552
  P-TDA-09(e): Security & Privacy Testing Throughout Development / Application Penetration Testing 555
P-TDA-10: Use of Live Data 556
  P-TDA-10(A): Use of Live Data / Test Data Integrity 557
P-TDA-11: Component Authenticity 557
  P-TDA-11(A): Component Authenticity / Anti-Counterfeit Training 558
THREAT MANAGEMENT (TPM) PROCEDURES

P-TPM-01: THIRD-PARTY MANAGEMENT
P-TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS
P-TPM-03: SUPPLY CHAIN PROTECTION
  P-TPM-03(a): SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES, TOOLS & METHODS
  P-TPM-03(b): SUPPLY CHAIN PROTECTION | LIMIT POTENTIAL HARM
  P-TPM-03(c): SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES
P-TPM-04: THIRD-PARTY SERVICES
  P-TPM-04(a): THIRD-PARTY SERVICES | THIRD-PARTY RISK ASSESSMENTS & APPROVALS
  P-TPM-04(b): THIRD-PARTY SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS & SERVICES
  P-TPM-04(c): THIRD-PARTY SERVICES | CONFLICT OF INTERESTS
  P-TPM-04(d): THIRD-PARTY SERVICES | THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS
P-TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS
P-TPM-06: THIRD-PARTY PERSONNEL SECURITY
P-TPM-07: MONITORING FOR THIRD-PARTY INFORMATION DISCLOSURE
P-TPM-08: REVIEW OF THIRD-PARTY SERVICES
P-TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION
P-TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES
P-TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES

THREAT MANAGEMENT (THR) PROCEDURES

P-THR-01: THREAT AWARENESS PROGRAM
P-THR-02: INDICATORS OF EXPOSURE (IOE)
P-THR-03: THREAT INTELLIGENCE FEEDS
P-THR-04: INSIDER THREAT PROGRAM
P-THR-05: INSIDER THREAT AWARENESS

VULNERABILITY & PATCH MANAGEMENT (VPM) PROCEDURES

P-VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM
  P-VPM-01(a): VULNERABILITY & PATCH MANAGEMENT PROGRAM | ESTABLISH VULNERABILITY MANAGEMENT SCOPE
P-VPM-02: VULNERABILITY REMEDIATION PROCESS
P-VPM-03: VULNERABILITY RANKING
P-VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES
  P-VPM-04(a): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES | STABLE VERSIONS
  P-VPM-04(b): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES | FLAW REMEDIATION WITH PERSONAL DATA (PD)
P-VPM-05: SOFTWARE PATCHING
  P-VPM-05(a): SOFTWARE PATCHING | CENTRALIZED MANAGEMENT
  P-VPM-05(b): SOFTWARE PATCHING | AUTOMATED REMEDIATION STATUS
  P-VPM-05(c): SOFTWARE PATCHING | TIME TO REMEDIATE / BENCHMARKS FOR CORRECTIVE ACTION
  P-VPM-05(d): SOFTWARE PATCHING | AUTOMATED SOFTWARE & FIRMWARE UPDATES
  P-VPM-05(e): SOFTWARE PATCHING | REMOVAL OF PREVIOUS VERSIONS
P-VPM-06: VULNERABILITY SCANNING
  P-VPM-06(a): VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY
  P-VPM-06(b): VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE
  P-VPM-06(c): VULNERABILITY SCANNING | PRIVILEGED ACCESS
  P-VPM-06(d): VULNERABILITY SCANNING | TRENDS AND TRENDS ANALYSIS
  P-VPM-06(e): VULNERABILITY SCANNING | REVIEW HISTORICAL AUDIT LOGS
**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.
  - 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 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 **SOC analyst** is responsible for performing daily log reviews, evaluating anomalous activities and responding to potential incidents in accordance with the organization’s Incident Response Plan (IRP).

**OVERVIEW**

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

**CUSTOMIZATION GUIDANCE**

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

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

**VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES**

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

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

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

Procedures should be both clearly-written and concise.
- Procedure documentation is meant to provide evidence of due diligence that standards are complied with.
- Well-managed procedures are critical to a security program, since procedures represent 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. 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 assigned to the End User Computing (EUC) team.
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
  - **Example:** Generally, system hardening is an “as needed” process that happens when new operating systems are released or when new technology is purchased. However, there should still be an annual review to ensure that appropriate baseline configurations exist and are current to what is deployed at ACME.
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
  - **Example:** The scope affects the entire company. Any deviations to the secure baselines are handled on an individual basis.
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
  - **Example:** Baseline configurations, benchmarks and STIGs are located on server XYZ123 in the folder called “Secure Baselines” and it is available for read-only for all users.
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
  - **Example:** There are no SLAs associated with baseline configurations.
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?
  - **Example:** The following classes of systems and applications are in scope for this procedure:
    - Server-Class Systems
    - Workstation-Class Systems
    - Network Devices
    - Databases

---

Control: 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.
SUPPORTING POLICIES & STANDARDS
While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge’s Digital Security Program (DSP) that contains policies, control objectives, standards and guidelines. It also directly maps to the Secure Controls Framework (SCF) for cybersecurity and privacy controls.

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

Cybersecurity Documentation Hierarchy
P-GOV-08: DEFINED BUSINESS CONTEXT & MISSION

Control: Mechanisms exist to define the context of its business model and document the mission of the organization.

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

(1) Researches, establishes and documents:
   a. ACME’s business model.
   b. ACME’s corporate mission statement so that cybersecurity-related objectives can be tied back to strategic concerns.
   c. Strength, Weakness, Opportunities & Threats (SWOT) analysis to define external and internal issues that are relevant and that affect the organization’s ability to achieve ACME’s mission (e.g., industry drivers, relevant regulations, basis for competition, etc.).

(2) Prioritizes the objectives and activities necessary to support ACME’s corporate mission in a cybersecurity and privacy-specific business plan that takes a multi-year approach to documenting:
   a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
   b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
   c. Resource requirements.
   d. Cybersecurity and privacy specific:
      i. Vision.
      ii. Mission.
      iii. Strategy.
   e. Prioritized objectives to accomplish the business plan.

(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-09: DEFINED CONTROL OBJECTIVES

Control: Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization’s internal control system.

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

(1) Researches, establishes and documents the appropriate internal control system for both cybersecurity and privacy controls that supports ACME’s applicable statutory, regulatory and/or contractual obligations.

(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.
Control: Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

1. Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.

2. Enables NTP for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.7

3. Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
   a. time.nist.gov 192.43.244.18 [primary].

P-MON-07: Time Stamps

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

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

Control: Mechanisms exist to configure systems to use internal system clocks to generate time stamps for audit records.
b. time-nw.nist.gov 131.107.13.100 [alternate].

(4) 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.

(5) If necessary, requests corrective action to address identified deficiencies.

(6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.

(7) If necessary, documents the results of corrective action and notes findings.

(8) If necessary, requests additional corrective action to address unremediated deficiencies.

P-MON-07(A): TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

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

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

Control: Mechanisms exist to synchronize internal system clocks with an authoritative time source.

**Procedure / Control Activity:** System Administrator [OM ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.

(2) Enables NTP is the Internet standard protocol for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.\(^8\)

(3) Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
   a. time.nist.gov 192.43.244.18 [primary].
   b. time-nw.nist.gov 131.107.13.100 [alternate].

(4) 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.

(5) If necessary, requests corrective action to address identified deficiencies.

(6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.

(7) If necessary, documents the results of corrective action and notes findings.

(8) If necessary, requests additional corrective action to address unremediated deficiencies.

P-MON-08: PROTECTION OF AUDIT INFORMATION

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

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure’s tasks

\(^8\) http://tycho.usno.navy.mil/ntp.html
P-HRS-13: IDENTIFY CRITICAL SKILLS & GAPS

Control: Mechanisms exist to evaluate the critical cybersecurity and privacy skills needed to support the organization’s mission and identify gaps that exist.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

(1) Conducts a critical skills inventory that:
   a. Analyzes the appropriate skills that are required to support the organization’s mission and business functions;
   b. Documents competencies necessary to define critical skills;
   c. Inventories the current technology staff for the identified critical skills;
   d. Documents the gap that exists in current versus needed critical skills;
   e. Proposes a solution to address the critical skills shortfall.

(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-HRS-13(a): IDENTIFY CRITICAL SKILLS & GAPS | REMEDIATE IDENTIFIED SKILLS DEFICIENCIES

Control: Mechanisms exist to remediate critical skills deficiencies necessary to support the organization’s mission and business functions.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

(1) Remediate critical skills deficiencies by:
   a. Resourcing new hires;
   b. Outsourcing the responsibilities to a competent third-party;
   c. Reassigning and training existing staff; and/or
   d. Creating new positions with higher level skill requirements.

(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-HRS-13(b): IDENTIFY CRITICAL SKILLS & GAPS | IDENTIFY VITAL CYBERSECURITY & PRIVACY STAFF

Control: Mechanisms exist to identify vital cybersecurity & privacy staff.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

(1) Identifies the objectives and activities necessary to support ACME’s corporate mission:
   a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
   b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
   c. Resource requirements.
   d. Cybersecurity and privacy specific:
      i. Vision.
      ii. Mission.
      iii. Strategy.
e. Prioritized objectives to accomplish the business plan.

2. Identifies critical staff by:
   a. Identifying vital cybersecurity & privacy staff;
   b. Documenting the role, function, responsibility and reasons that supports their designation as vital;
   c. Where possible, identifying staff that can backfill vital roles.

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-HRS-13(c): IDENTIFY CRITICAL SKILLS & GAPS | ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & PRIVACY STAFF**

**Control:** Mechanisms exist to establish redundancy for vital cybersecurity & privacy staff.

**Procedure / Control Activity:** The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

1. Conducts a critical skills inventory that:
   a. Analyzes the appropriate skills that are required to support the organization’s mission and business functions;
   b. Documents competencies necessary to define critical skills;
   c. Inventories the current technology staff for the identified critical skills;
   d. Documents the gap that exists in current versus needed critical skills;

2. Designates roles that require redundancy.

3. Identifies a primary and alternate staff member for vital cybersecurity & privacy roles.

4. Proposes a solution to address any redundancy shortfalls.

5. 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.

6. If necessary, requests corrective action to address identified deficiencies.

7. If necessary, validates corrective action occurred to appropriately remediate deficiencies.

8. If necessary, documents the results of corrective action and notes findings.

9. If necessary, requests additional corrective action to address unremediated deficiencies.

**P-HRS-13(d): IDENTIFY CRITICAL SKILLS & GAPS | PERFORM SUCCESSION PLANNING**

**Control:** Mechanisms exist to perform succession planning for vital cybersecurity & privacy roles.

**Procedure / Control Activity:** The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

1. Manages succession planning as an extensive and systematic activity that:
   a. Maintains documented roles and responsibilities for vital cybersecurity & privacy staff positions;
   b. Works with senior leaders who responsible those vital cybersecurity & privacy staff positions to develop succession plans;
   c. Works with identified staff members to provide training and/or guidance on steps needed to successfully move into the new role if succession plans must be implemented to help ensure a smooth transition.

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-IRO-02(c): INCIDENT HANDLING | DYNAMIC RECONFIGURATION

Control: Automated mechanisms exist to dynamically reconfigure information system components as part of the incident response capability.

Procedure / Control Activity: System Administrator [OM-ADM-001], in conjunction with Asset Owner [XX-AST-001], Crisis Management Specialist [XX-CON-001], Disaster Recovery Team Leader [XX-CON-003] and Business Continuity Team Leader [XX-CON-005]:

1. Develops specific use cases where dynamic reconfiguration is appropriate that includes:
   a. Stopping an active attack;
   b. Misdirecting attackers; and
   c. Isolating systems, thus limiting the extent of the damage from breaches or compromises.

2. Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms to employ automated mechanisms that enable dynamic reconfiguration of systems as part of incident response remediation actions that includes:
   a. Changes to router or firewall Access Control Lists (ACLs);
   b. Intrusion Detection / Prevention System (IDS/IPS) parameters.

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-IRO-02(d): INCIDENT HANDLING | CONTINUITY OF OPERATIONS

Control: Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.

Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02] and Cyber Defense Incident Responder [PR-CIR-001]:

1. Leverages the Integrated Incident Response Program (IIRP) to categorize cybersecurity incidents based on each category’s potential to escalate and different handling procedures:

<table>
<thead>
<tr>
<th>#</th>
<th>Threat</th>
<th>Category</th>
<th>Category Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Training</td>
<td>Simulated Incident (Training &amp; Exercises)</td>
<td>This category is used during exercises and approved testing of internal/external network defenses or responses.</td>
</tr>
<tr>
<td>1</td>
<td>Illegal Content</td>
<td></td>
<td>This category is used for any data that is illegal to have in possession.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Illegal Content or Activities</td>
<td>This includes illegal content such as child pornography or classified information on unclassified systems.</td>
</tr>
<tr>
<td>2</td>
<td>Criminal Conduct</td>
<td></td>
<td>This category is used for any incident that would be considered criminal conduct.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Criminal Conduct</td>
<td>This includes embezzlement, corporate espionage, terrorism/national security threats, fraud, violence or other conduct that would constitute a criminal felony or misdemeanor charge.</td>
</tr>
<tr>
<td>3</td>
<td>Safety</td>
<td>Technology Compromise</td>
<td>This category is used for any incident that has safety implications from the compromise of the technology to be used in a manner it was not designed for.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This includes categories of technologies that includes Operational Technology (OT) and Internet of Things (IoT).</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>Breach of Sensitive Data</td>
<td>This category is used for any incident that has involves the unauthorized disclosure or compromise of sensitive data. This includes sensitive Personal Data (PD) and Intellectual Property (IP).</td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Malware</td>
<td></td>
<td>This category is used for malware-related incidents. Any software code intentionally created or introduced into multiple systems for the distinct purpose of causing hard or loss to the computer system, its data or other resources (e.g., spyware, adware, viruses, Trojans, worms, etc.).</td>
</tr>
<tr>
<td>6</td>
<td>Nefarious Activity</td>
<td>Host / Application Compromise</td>
<td>This is a known or suspected compromise that is not directly related to malware. A successful event of this nature means the attacker has total control over the host or application and access to any and all data stored on it or on systems that trust the compromised host or application. This may be from a privilege escalation attack.</td>
</tr>
<tr>
<td>7</td>
<td>Denial of Service (DoS)</td>
<td>Denial of Service (DoS)</td>
<td>This is a known or suspected Denial of Service (DoS) attack. A successful event of this nature means the attacker(s) successfully denied access to either the entire network, a portion of the network or to critical service(s) / website(s).</td>
</tr>
<tr>
<td>8</td>
<td>Lost / Stolen Asset</td>
<td>Lost / Stolen IT Asset</td>
<td>This category is used to respond to any lost or stolen IT equipment (e.g., laptops, tablets, computers, servers, media, tapes, etc.)</td>
</tr>
<tr>
<td>9</td>
<td>Poor Security Practice</td>
<td>Poor Security Practice</td>
<td>This category is used for any suspected incident involving misconfigurations, poor cybersecurity practices &amp; policy violations.</td>
</tr>
<tr>
<td>10</td>
<td>Unknown / Other (Under Investigation)</td>
<td>Unknown / Other (Under Investigation)</td>
<td>This category is used if the situation is unclear and categorization cannot be made. This is meant to be a &quot;placeholder&quot; category until the threat or situation is investigated and a final determination has been made, so that the incident can be properly categorized.</td>
</tr>
</tbody>
</table>

(2) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms to employ the IIRP to ensure users understand the different categories of incidents and the actions required to be taken, per ACME’s Incident Response Plan (IRP).

(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-PES-03(c): PHYSICAL ACCESS CONTROL | PHYSICAL ACCESS LOGS**

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

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

---

**Control:** Physical access control mechanisms exist to generate a log entry for each access through controlled ingress and egress points.

**Procedure / Control Activity:** Physical Security Specialist [XX-PES-001]:

1. Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure access control systems to log the following information:
   a. Physical location of the access;
   b. Direction of access, if possible (e.g., ingress or egress);
   c. Identity of the person accessing the location; and
   d. Indication of success or failure.
2. Uses a visitor log to maintain a physical audit trail of visitor activity:
   a. At a minimum, document the visitor’s name, the company represented, and the onsite personnel authorizing physical access; and
   b. Retain this log for a minimum of three months, unless otherwise restricted by law.
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. Distributed 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-PES-03(d): PHYSICAL ACCESS CONTROL | ACCESS TO INFORMATION SYSTEMS**

**Control:** Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive data, in addition to the physical access controls for the facility.

**Procedure / Control Activity:** Asset Owner [XX-AST-001], in conjunction with Physical Security Specialist [XX-PES-001] and Physical Security Manager [XX-PES-002]:

1. Implements appropriate administrative, physical and technical means to enforce physical access authorizations to information systems in addition to the physical access controls.
2. Develops unique physical security zones to determine specific areas that are more vulnerable to unauthorized use, theft or viewing of data where enhanced physical safeguards should be implemented:
   a. Facilities management implements physical access authorization mechanisms to secure workspaces, such as:
      i. Proximity badges; or
      ii. Personalized PIN pad
   b. Line supervisors and manage facilitate “clean desk” requirements for all work areas to ensure media containing sensitive data is properly secured when the workspace is not occupied, including:
      i. Filing cabinets, lockable drawers / overhead cabinets, storage rooms and any other storage unit containing sensitive data will be locked when not in use; and