WRITTEN INFORMATION SECURITY PROGRAM (WISP)

[NIST SP 800 53 Rev4 Low-Moderate Baselines]

ACME Business Solutions, LLC
# Table of Contents

## Written Information Security Program (WISP) Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>12</td>
</tr>
<tr>
<td>Purpose</td>
<td>12</td>
</tr>
<tr>
<td>Scope &amp; Applicability</td>
<td>13</td>
</tr>
<tr>
<td>Policy Overview</td>
<td>13</td>
</tr>
<tr>
<td>Violations</td>
<td>13</td>
</tr>
<tr>
<td>Exceptions</td>
<td>13</td>
</tr>
<tr>
<td>Updates</td>
<td>13</td>
</tr>
<tr>
<td>Key Terminology</td>
<td>14</td>
</tr>
</tbody>
</table>

## Cybersecurity Program Structure

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies, Standards, Procedures &amp; Guidelines Structure</td>
<td>16</td>
</tr>
<tr>
<td>Cybersecurity Control Objectives</td>
<td>16</td>
</tr>
<tr>
<td>Cybersecurity Program Activities</td>
<td>18</td>
</tr>
<tr>
<td>Cybersecurity Considerations For Protecting Systems</td>
<td>18</td>
</tr>
</tbody>
</table>

## Management Controls

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Management (PM)</td>
<td>19</td>
</tr>
<tr>
<td>PM-1: Information Security Program Plan</td>
<td>19</td>
</tr>
<tr>
<td>PM-2: Senior Information Security Officer</td>
<td>19</td>
</tr>
<tr>
<td>PM-3: Information Security Resources</td>
<td>20</td>
</tr>
<tr>
<td>PM-4: Plan of Action &amp; Milestones (POA&amp;M) Process (Vulnerability Remediation)</td>
<td>20</td>
</tr>
<tr>
<td>PM-5: Information System Inventory</td>
<td>20</td>
</tr>
<tr>
<td>PM-6: Information Security Measures of Performance</td>
<td>20</td>
</tr>
<tr>
<td>PM-7: Enterprise Architecture</td>
<td>21</td>
</tr>
<tr>
<td>PM-8: Critical Infrastructure Plan (CIP)</td>
<td>21</td>
</tr>
<tr>
<td>PM-9: Risk Management Strategy</td>
<td>21</td>
</tr>
<tr>
<td>PM-10: Security Authorization Process</td>
<td>22</td>
</tr>
<tr>
<td>PM-11: Mission / Business Process Definition</td>
<td>22</td>
</tr>
<tr>
<td>PM-12: Insider Threat Program</td>
<td>22</td>
</tr>
<tr>
<td>PM-13: Information Security Workforce</td>
<td>22</td>
</tr>
<tr>
<td>PM-14: Testing, Training &amp; Monitoring</td>
<td>23</td>
</tr>
<tr>
<td>PM-15: Contacts With Security Groups &amp; Associations</td>
<td>23</td>
</tr>
<tr>
<td>PM-16: Threat Awareness Program</td>
<td>24</td>
</tr>
</tbody>
</table>

## Security Assessments & Authorization (CA)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-1: Security Assessment &amp; Authorization Policy &amp; Procedures</td>
<td>25</td>
</tr>
<tr>
<td>CA-2: Security Assessments</td>
<td>25</td>
</tr>
<tr>
<td>CA-2(1): Security Assessments Independent Assessors</td>
<td>26</td>
</tr>
<tr>
<td>CA-2(2): Security Assessments Specialized Assessments</td>
<td>26</td>
</tr>
<tr>
<td>CA-2(3): Security Assessments External Organizations</td>
<td>26</td>
</tr>
<tr>
<td>CA-3: System Interconnections</td>
<td>26</td>
</tr>
<tr>
<td>CA-3(3): System Interconnections Unclassified Non-National Security System Connections</td>
<td>27</td>
</tr>
<tr>
<td>CA-3(5): System Interconnections Restrictions on External System Connections</td>
<td>27</td>
</tr>
<tr>
<td>CA-5: Plan of Action &amp; Milestones (POA&amp;M)</td>
<td>27</td>
</tr>
<tr>
<td>CA-6: Security Authorization</td>
<td>27</td>
</tr>
<tr>
<td>CA-7: Continuous Monitoring</td>
<td>28</td>
</tr>
<tr>
<td>CA-7(1): Continuous Monitoring Independent Assessment</td>
<td>28</td>
</tr>
<tr>
<td>CA-8: Penetration Testing</td>
<td>28</td>
</tr>
<tr>
<td>CA-8(1): Penetration Testing Independent Penetration Agent or Team</td>
<td>29</td>
</tr>
<tr>
<td>CA-9: Internal System Connections</td>
<td>29</td>
</tr>
</tbody>
</table>

## Planning (PL)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL-1: Security Planning Policy &amp; Procedures</td>
<td>30</td>
</tr>
<tr>
<td>PL-2: System Security Plan (SSP)</td>
<td>30</td>
</tr>
<tr>
<td>PL-2(3): System Security Plan Plan / Coordinate with Other Organizational Entities</td>
<td>31</td>
</tr>
<tr>
<td>PL-4: Rules of Behavior</td>
<td>32</td>
</tr>
<tr>
<td>PL-4(1): Rules Of Behavior</td>
<td>32</td>
</tr>
<tr>
<td><strong>PL-7</strong>: Security Concept of Operations</td>
<td>33</td>
</tr>
<tr>
<td><strong>PL-8</strong>: Information Security Architecture</td>
<td>33</td>
</tr>
<tr>
<td><strong>PL-9</strong>: Central Management</td>
<td>33</td>
</tr>
</tbody>
</table>

**Risk Assessment (RA)**

RA-1: Risk Assessment Policy & Procedures
RA-2: Security Categorization
RA-3: Risk Assessment
RA-5: Vulnerability Scanning
  - RA-5(1): Vulnerability Scanning | Update Tool Capability
  - RA-5(2): Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified
  - RA-5(3): Vulnerability Scanning | Breadth / Depth of Coverage
  - RA-5(4): Vulnerability Scanning | Privileged Access
  - RA-5(6): Vulnerability Scanning | Automated Trend Analysis
  - RA-5(8): Vulnerability Scanning | Review Historical Audit Logs
RA-6: Technical Surveillance Countermeasures Security

**System & Service Acquisition (SA)**

SA-1: System & Services Acquisition Policy & Procedures
SA-2: Allocation of Resources
SA-3: System Development Life Cycle (SDLC)
SA-4: Acquisition Process
  - SA-4(8): Acquisition Process | Continuous Monitoring Plan
  - SA-4(9): Acquisition Process | Functions, Ports, Protocols & Services In Use
  - SA-4(10): Acquisition Process | Use of Approved PIV Products
SA-5: Information System Documentation
SA-6: Software Usage Restrictions [Withdrawn from NIST 800-53 Rev4]
SA-7: User Installed Software [Withdrawn from NIST 800-53 Rev4]
SA-8: Security Engineering Principles
SA-9: External Information System Services
  - SA-9(1): External Information System Services | Risk Assessments & Organizational Approvals
  - SA-9(2): External Information System Services | Identification Of Functions, Ports, Protocols & Services
  - SA-9(4): External Information System Services | Consistent Interests of Consumers and Providers
  - SA-9(5): External Information System Services | Processing, Storage and Service Location
SA-10: Developer Configuration Management
SA-10(1): Developer Configuration Management | Software / Firmware Integrity Verification
SA-11: Developer Security Testing
SA-12: Supply Chain Protection
SA-13: Trustworthiness
SA-14: Criticality Analysis
SA-15: Development Process, Standards & Tools
SA-16: Developer-Provided Training
SA-17: Developer Security Architecture & Design
SA-18: Tamper Resisitance & Detection
SA-19: Component Authenticity
SA-20: Customized Development of Critical Components
SA-21: Developer Screening
SA-22: Unsupported System Components

**Operational Controls**

**Awareness & Training (AT)**

AT-1: Security Awareness & Training Policy & Procedures
AT-2: Security Awareness Training
| AT-2(2): Security Awareness Training | Insider Threat   | 52  |
| AT-3: ROLE-BASED SECURITY TRAINING |                           | 52  |
| AT-4: SECURITY TRAINING RECORDS   |                           | 53  |
| AT-5: CONTACTS WITH SECURITY GROUPS & ASSOCIATIONS [WITHDRAWN FROM NIST 800-53 REV4] |                           | 53  |
| CONTINGENCY PLANNING (CP)         |                           | 54  |
| CP-1: CONTINGENCY PLANNING POLICY & PROCEDURES |                           | 54  |
| CP-2: CONTINGENCY PLAN            |                           | 54  |
|   CP-2(1): Contingency Plan | Coordinate with Related Plans | 55  |
|   CP-2(2): Contingency Plan | Capacity Planning          | 55  |
|   CP-2(3): Contingency Plan | Resume Essential Missions / Business Functions | 55  |
|   CP-2(8): Contingency Plan | Identify Critical Assets   | 55  |
| CP-3: CONTINGENCY TRAINING       |                           | 56  |
| CP-4: CONTINGENCY PLAN TESTING   |                           | 56  |
|   CP-4(1): Contingency Plan Testing | Coordinate with Related Plans | 56  |
| CP-5: CONTINGENCY PLAN UPDATE [WITHDRAWN FROM NIST 800-53 REV4] |                           | 57  |
| CP-6: ALTERNATE STORAGE SITE      |                           | 57  |
|   CP-6(1): Alternate Storage Site | Separation from Primary Site | 57  |
|   CP-6(3): Alternate Storage Site | Accessibility           | 57  |
| CP-7: ALTERNATE PROCESSING SITE   |                           | 57  |
|   CP-7(1): Alternate Processing Site | Separation from Primary Site | 57  |
|   CP-7(2): Alternate Processing Site | Accessibility           | 57  |
|   CP-7(3): Alternate Processing Site | Priority of Service    | 58  |
| CP-8: TELECOMMUNICATIONS SERVICES |                           | 58  |
|   CP-8(1): Telecommunications Services | Priority of Service Provisions | 59  |
|   CP-8(2): Telecommunications Services | Single Points of Failure | 59  |
| CP-9: INFORMATION SYSTEM BACKUP   |                           | 59  |
|   CP-9(1): Information System Backup | Testing for Reliability & Integrity | 60  |
|   CP-9(3): Information System Backup | Separate Storage for Critical Information | 61  |
| CP-10: INFORMATION SYSTEM RECOVERY & RECONSTITUTION |                           | 61  |
|   CP-10(2): Information System Recovery & Reconstitution | Transaction Recovery | 61  |
| CP-11: ALTERNATE COMMUNICATIONS PROTOCOLS |                           | 61  |
| CP-12: SAFE MODE                 |                           | 62  |
| CP-13: ALTERNATIVE SECURITY MEASURES |                           | 62  |
| INCIDENT RESPONSE (IR)           |                           | 63  |
| IR-1: INCIDENT RESPONSE POLICY & PROCEDURES |                           | 63  |
| IR-2: INCIDENT RESPONSE TRAINING |                           | 63  |
| IR-3: INCIDENT RESPONSE TESTING  |                           | 63  |
|   IR-3(2): Incident Response Testing | Coordination with Related Plans | 64  |
| IR-4: INCIDENT HANDLING          |                           | 64  |
|   IR-4(1): Incident Handling | Automated Incident Handling Processes | 64  |
| IR-5: INCIDENT MONITORING        |                           | 64  |
| IR-6: INCIDENT REPORTING         |                           | 65  |
|   IR-6(1): Incident Reporting | Automated Reporting       | 65  |
| IR-7: INCIDENT REPORTING ASSISTANCE |                           | 66  |
|   IR-7(1): Incident Reporting Assistance | Automation Support of Availability of Information / Support | 66  |
|   IR-7(2): Incident Reporting Assistance | Coordination With External Providers | 66  |
| IR-8: INCIDENT RESPONSE PLAN (IRP) |                           | 66  |
| IR-9: INFORMATION SPILLAGE RESPONSE |                           | 67  |
|   IR-9(1): Information Spillage Response | Responsible Personnel  | 68  |
|   IR-9(2): Information Spillage Response | Training | 68  |
|   IR-9(3): Information Spillage Response | Post-Spill Operations | 68  |
|   IR-9(4): Information Spillage Response | Exposure to Unauthorized Personnel | 68  |
| IR-10: INTEGRATED INFORMATION SECURITY ANALYSIS TEAM |                           | 68  |
| MEDIA PROTECTION (MP)            |                           | 69  |
| MP-1: MEDIA PROTECTION POLICY & PROCEDURES |                           | 69  |
| MP-2: MEDIA ACCESS               |                           | 69  |
| MP-3: MEDIA MARKING              |                           | 70  |
| MP-4: MEDIA STORAGE              |                           | 70  |

**INTERNAL USE**

*Access Limited to Internal Use Only*

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

Page 4 of 183
MP-5: MEDIA TRANSPORT
  MP-5(4): Media Transport | Cryptographic Protection (Encrypting Data In Storage Media)
MP-6: MEDIA SANITIZATION
  MP-6(2): Media Sanitization | Equipment Testing
MP-7: MEDIA USE
  MP-7(1): Media Use | Prohibit Use Without Owner
MP-8: MEDIA DOWNGRADING

PERSONNEL SECURITY (PS)
  PS-1: PERSONNEL SECURITY POLICY & PROCEDURES
  PS-2: POSITION RISK DESIGNATION (POSITION CATEGORIZATION)
  PS-3: PERSONNEL SCREENING
    PS-3(3): Personnel Screening | Information With Special Protection Measures
  PS-4: PERSONNEL TERMINATION
  PS-5: PERSONNEL TRANSFER
  PS-6: ACCESS AGREEMENTS
  PS-7: THIRD-PARTY PERSONNEL SECURITY
  PS-8: PERSONNEL SANCTIONS

PHYSICAL & ENVIRONMENTAL PROTECTION (PE)
  PE-1: PHYSICAL & ENVIRONMENTAL PROTECTION POLICY & PROCEDURES
  PE-2: PHYSICAL ACCESS AUTHORIZATIONS
  PE-3: PHYSICAL ACCESS CONTROL
  PE-4: ACCESS CONTROL FOR TRANSMISSION MEDIUM
  PE-5: ACCESS CONTROL FOR OUTPUT DEVICES
  PE-6: MONITORING PHYSICAL ACCESS
    PE-6(1): Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment
  PE-7: VISITOR CONTROL [WITHDRAWN FROM NIST 800-53 REV4]
  PE-8: VISITOR ACCESS RECORDS
  PE-9: POWER EQUIPMENT & POWER CABLING
  PE-10: EMERGENCY SHUTOFF
  PE-11: EMERGENCY POWER
  PE-12: EMERGENCY LIGHTING
  PE-13: FIRE PROTECTION
    PE-13(2): Fire Protection | Fire Suppression Devices
    PE-13(3): Fire Protection | Automatic Fire Suppression
  PE-14: TEMPERATURE & HUMIDITY CONTROLS
    PE-14(2): Temperature & Humidity Controls | Monitoring with Alarms / Notifications
  PE-15: WATER DAMAGE PROTECTION
  PE-16: DELIVERY & REMOVAL
  PE-17: ALTERNATE WORK SITE
  PE-18: LOCATION OF INFORMATION SYSTEM COMPONENTS
  PE-19: INFORMATION LEAKAGE
  PE-20: ASSET MONITORING & TRACKING

TECHNICAL CONTROLS

Access Control (AC)
  AC-1: ACCESS CONTROL POLICY & PROCEDURES
  AC-2: ACCOUNT MANAGEMENT
    AC-2(1): Account Management | Automated System Account Management
    AC-2(2): Account Management | Removal of Temporary / Emergency Accounts
    AC-2(3): Account Management | Disable Inactive Accounts
    AC-2(4): Account Management | Automated Audit Actions
    AC-2(5): Account Management | Inactivity Logout
    AC-2(7): Account Management | Role Based Schemes (Role-Based Access Control (RBAC))
    AC-2(9): Account Management | Restrictions on Shared Groups / Accounts
    AC-2(10): Account Management | Shared / Group Account Credential Termination
    AC-2(12): Account Management | Account Monitoring / Atypical Usage
  AC-3: ACCESS ENFORCEMENT
  AC-4: INFORMATION FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)
    AC-4(21): Information Flow Enforcement | Physical / Logical Separation for Information Flows
AC-5: Separation of Duties
AC-6: Least Privilege
   AC-6(1): Least Privilege | Authorize Access to Security Functions
   AC-6(2): Least Privilege | Non-Privileged Access for Non-Security Functions
   AC-6(5): Least Privilege | Privileged Accounts
   AC-6(9): Least Privilege | Auditing Use of Privileged Functions
   AC-6(10): Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7: Unsuccessful Login Attempts
AC-8: System Use Notification (Logon Banner)
AC-9: Previous Logon Notification
AC-10: Concurrent Session Control
   AC-11(1): Session Lock | Pattern-Hiding Displays
AC-12: Least Privilege | Non-Privileged Access for Non-Security Functions
AC-13: Least Privilege | Auditing Use of Privileged Functions
AC-14: Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions
AC-15: Least Privilege | Access by Subset of Privileged Users
AC-16: Security Attributes
AC-17: Remote Access
   AC-17(1): Remote Access | Automated Monitoring / Control
   AC-17(2): Remote Access | Protection of Confidentiality / Integrity Using Encryption
   AC-17(3): Remote Access | Managed Access Control Points
   AC-17(4): Remote Access | Privileged Commands & Access
   AC-17(9): Remote Access | Disconnect / Disable Remote Access
AC-18: Wireless Access
AC-19: Access Control For Mobile Devices
   AC-19(5): Access Control For Mobile Devices | Full Device / Container-Based Encryption
AC-20: Use of External Information Systems
   AC-20(1): Use of External Information Systems | Limits of Authorized Use
   AC-20(2): Use of External Information Systems | Portability of Portable Storage Devices
AC-21: Information Sharing
AC-22: Publicly Accessible Content
AC-23: Data Mining Protection
AC-24: Access Control Decisions
AC-25: Reference Monitor

Audit & Accountability (AU)
AU-1: Audit & Accountability Policy & Procedures
AU-2: Auditable Events
   AU-2(3): Auditable Events | Reviews & Updates
AU-3: Content of Audit Records
   AU-3(1): Content Of Audit Records | Additional Audit Information
AU-4: Audit Storage Capacity
AU-5: Response To Audit Processing Failures
AU-6: Audit Review, Analysis & Reporting
   AU-6(1): Audit Review, Analysis & Reporting | Process Integration
   AU-6(3): Audit Review, Analysis & Reporting | Correlate Audit Repositories
AU-7: Audit Reduction & Report Generation
   AU-7(1): Audit Reduction & Report Generation | Automatic Processing
AU-8: Time Stamps
   AU-8(1): Time Stamps | Synchronization With Authoritative Time Source
AU-9: Protection of Audit Information
   AU-9(2): Protection of Audit Information | Audit Backup on Separate Physical Systems / Components
   AU-9(4): Protection of Audit Information | Access by Subset of Privileged Users
AU-10: Non-Repudiation
AU-11: Audit Record Retention
   AU-11(1): Audit Record Retention | Long-Term Retrieval Capability
AU-12: Audit Generation
AU-13: MONITORING FOR INFORMATION DISCLOSURE
AU-14: SESSION AUDIT
AU-15: ALTERNATE AUDIT CAPABILITY
AU-16: CROSS-ORGANIZATIONAL AUDITING

CONFIGURATION MANAGEMENT (CM)

CM-1: CONFIGURATION MANAGEMENT POLICY & PROCEDURES
CM-2: BASELINE CONFIGURATIONS
   CM-2(1): Baseline Configuration | Reviews & Updates
   CM-2(2): Baseline Configuration | Automation Support for Accuracy / Currency
   CM-2(3): Baseline Configuration | Retention Of Previous Configurations
   CM-2(7): Baseline Configuration | Configure Systems, Components or Devices for High-Risk Areas

CM-3: CONFIGURATION CHANGE CONTROL
   CM-3(2): Configuration Change Control | Test, Validate & Document Changes

CM-4: SECURITY IMPACT ANALYSIS
CM-5: ACCESS RESTRICTION FOR CHANGE
   CM-5(1): Access Restrictions For Change | Automated Access Enforcement / Auditing
   CM-5(3): Access Restrictions For Change | Signed Components
   CM-5(5): Access Restrictions For Change | Limit Production / Operational Privileges (Incompatible Roles)

CM-6: CONFIGURATION SETTINGS
CM-6(1): Configuration Settings | Automated Central Management / Application / Verification

CM-7: LEAST FUNCTIONALITY
   CM-7(1): Least Functionality | Periodic Review
   CM-7(2): Least Functionality | Prevent Program Execution
   CM-7(4): Least Functionality | Unauthorized Software (Blacklisting)
   CM-7(5): Least Functionality | Authorized Software (Whitelisting)

CM-8: INFORMATION SYSTEM COMPONENT INVENTORY
   CM-8(1): Information System Component Inventory | Updates During Installations / Removals
   CM-8(3): Information System Component Inventory | Automated Unauthorized Component Detection
   CM-8(5): Information System Component Inventory | No Duplicate Accounting of Components

CM-9: CONFIGURATION MANAGEMENT PLAN
CM-10: SOFTWARE USAGE RESTRICTIONS
   CM-10(1): Software Usage Restrictions | Open Source Software
CM-11: USER-INSTALLED SOFTWARE

IDENTIFICATION & AUTHENTICATION (IA)

IA-1: IDENTIFICATION & AUTHENTICATION POLICY & PROCEDURES
IA-2: IDENTIFICATION & AUTHENTICATION (ORGANIZATIONAL USERS)
   IA-2(1): Identification & Authentication (Organizational Users) | Network Access to Privileged Accounts
   IA-2(2): Identification & Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
   IA-2(3): Identification & Authentication (Organizational Users) | Local Access to Privileged Accounts
   IA-2(5): Identification & Authentication (Organizational Users) | Group Authentication
   IA-2(8): Identification & Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant

   IA-2(9): Identification & Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant
   IA-2(12): Identification & Authentication (Organizational Users) | Acceptance of PIV Credentials

IA-3: DEVICE IDENTIFICATION & AUTHENTICATION
IA-4: IDENTIFIER MANAGEMENT (USER NAMES)
IA-4(4): Identifier Management | Identity User Status

IA-5: AUTHENTICATOR MANAGEMENT (PASSWORDS)
   IA-5(1): Authenticator Management | Password-Based Authentication
   IA-5(2): Authenticator Management | PKI-Based Authentication
   IA-5(3): Authenticator Management | In-Person or Trusted Third-Party Registration
   IA-5(4): Authenticator Management | Automated Support For Password Strength Determination
   IA-5(5): Authenticator Management | Change Authenticators Prior to Delivery
   IA-5(6): Authenticator Management | Protection of Authenticators
   IA-5(7): Authenticator Management | No Embedded Unencrypted Static Authenticators
   IA-5(11): Authenticator Management | Hardware Token-Based Authentication

INTERNAL USE
Access Limited to Internal Use Only

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)
IA-6: AUTHENTICATOR FEEDBACK 125
IA-7: CRYPTOGRAPHIC MODULE AUTHENTICATION 125
IA-8: IDENTIFICATION & AUTHENTICATION (NON-ORGANIZATIONAL USERS) 125
  IA-8(1): Identification & Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Organizations 126
  IA-8(2): Identification & Authentication (Non-Organizational Users) | Acceptance of Third-Party Credentials 126
  IA-8(3): Identification & Authentication (Non-Organizational Users) | Use of FICAM-Approved Products 126
  IA-8(4): Identification & Authentication (Non-Organizational Users) | Use of FICAM-Issued Profiles 126
IA-9: SERVICE PROVIDER IDENTIFICATION & AUTHENTICATION (VENDORS) 127
IA-10: ADAPTIVE IDENTIFICATION & AUTHENTICATION 127
IA-11: RE-AUTHENTICATION 127
MAINTENANCE (MA) 128
MA-1: MAINTENANCE POLICY & PROCEDURES 128
MA-2: CONTROLLED MAINTENANCE 128
MA-3: MAINTENANCE TOOLS 129
  MA-3(1): Maintenance Tools | Inspect Tools 129
  MA-3(2): Maintenance Tools | Inspect Media 129
  MA-3(3): Maintenance Tools | Prevent Unauthorized Removal 129
MA-4: NON-LOCAL MAINTENANCE 130
MA-5: MAINTENANCE PERSONNEL 130
MA-6: TIMELY MAINTENANCE 131
SYSTEM & COMMUNICATION PROTECTION (SC) 132
SC-1: SYSTEM & COMMUNICATION POLICY & PROCEDURES 132
SC-2: APPLICATION PARTITIONING 132
SC-3: SECURITY FUNCTION ISOLATION 133
SC-4: INFORMATION IN SHARED RESOURCES 133
SC-5: DENIAL OF SERVICE (DoS) PROTECTION 133
SC-6: RESOURCE PRIORITY 134
SC-7: BOUNDARY PROTECTION 134
  SC-7(3): Boundary Protection | Access Points 134
  SC-7(4): Boundary Protection | External Telecommunications Services 135
  SC-7(5): Boundary Protection | Deny by Default & Allow by Exception (Access Control List) 135
  SC-7(7): Boundary Protection | Prevent Split Tunneling for Remote Devices 135
  SC-7(8): Boundary Protection | Route Traffic To Authenticated Proxy Servers 135
  SC-7(12): Boundary Protection | Host-Based Protection 136
  SC-7(13): Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components (Security Subnet) 136
  SC-7(18): Boundary Protection | Fail Secure 136
SC-8: TRANSMISSION CONFIDENTIALITY AND INTEGRITY 136
  SC-8(1): Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection 137
SC-10: NETWORK DISCONNECT 137
SC-11: TRUSTED PATH 138
SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT & MANAGEMENT 138
  SC-12(2): Cryptographic Key Establishment & Management | Symmetric Keys 139
  SC-12(3): Cryptographic Key Establishment & Management | Asymmetric Keys 139
SC-13: USE OF CRYPTOGRAPHY 139
SC-14: PUBLIC ACCESS PROTECTION [WITHDRAWN FROM NIST 800-53 REV4] 139
SC-15: COLLABORATIVE COMPUTING DEVICES 139
SC-16: TRANSMISSION OF SECURITY ATTRIBUTES 140
SC-17: PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATES 140
SC-18: MOBILE CODE 140
SC-19: VOICE OVER INTERNET PROTOCOL (VOIP) 141
SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) 141
SC-21: SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) 142
SC-22: ARCHITECTURE & PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE 142
SC-23: SESSION AUTHENTICITY 142
SC-24: FAIL IN KNOWN STATE
SC-25: THIN NODES
SC-26: HONEYPOTS
SC-27: PLATFORM-INDEPENDENT APPLICATIONS
SC-28: ENCRYPTING DATA AT REST
   SC-28(1): Encrypting Data at Rest | Cryptographic Protection
SC-29: HETEROGENEITY
SC-30: CONCEALMENT & MISDIRECTION
SC-31: COVERT CHANNEL ANALYSIS
SC-32: INFORMATION SYSTEM PARTITIONING
SC-33: TRANSMISSION PREPARATION INTEGRITY [WITHDRAWN FROM NIST 800-53 REV4]
SC-34: NON-MODIFIABLE EXECUTABLE PROGRAMS
SC-35: HONECLIENTS
SC-36: DISTRIBUTED PROCESSING & STORAGE
SC-37: OUT-OF-BAND CHANNELS
SC-38: OPERATIONS SECURITY
SC-39: PROCESS ISOLATION
SC-40: WIRELESS LINK PROTECTION
SC-41: PORT & I/O DEVICE ACCESS
SC-42: SENSOR CAPABILITY & DATA
   SC-42(3): Sensor Capability & Data | Prohibit Use of Devices
SC-43: USAGE RESTRICTIONS
SC-44: DETONATION CHAMBERS

SYSTEM & INFORMATION INTEGRITY (SI) 150
SI-1: SYSTEM & INFORMATION INTEGRITY POLICY & PROCEDURES
SI-2: FLAW REMEDIATION (SOFTWARE PATCHING)
   SI-2(2): Flaw Remediation | Automated Flaw Remediation Status
   SI-2(3): Flaw Remediation | Time To Remediate Flaws / Benchmarks For Corrective Action
SI-3: MALICIOUS CODE PROTECTION (MALWARE)
   SI-3(1): Malicious Code Protection | Central Management
   SI-3(2): Malicious Code Protection | Automatic Updates
   SI-3(7): Malicious Code Protection | Nonsignature-Based Detection
SI-4: INFORMATION SYSTEM MONITORING
   SI-4(4): Information System Monitoring | Inbound & Outbound Communications Traffic
   SI-4(5): Information System Monitoring | System Generated Alerts
   SI-4(14): Information System Monitoring | Wireless Intrusion Detection
   SI-4(16): Information System Monitoring | Correlate Monitoring Information
   SI-4(23): Information System Monitoring | Host-Based Devices
SI-5: SECURITY ALERTS, ADVISORIES & DIRECTIVES
SI-6: SECURITY FUNCTIONALITY VERIFICATION
SI-7: SOFTWARE, Firmware & INFORMATION INTEGRITY
   SI-7(1): Software, Firmware & Information Integrity | Integrity Checks
   SI-7(7): Software, Firmware & Information Integrity | Integration of Detection & Response
SI-8: SPAM PROTECTION
   SI-8(1): Spam Protection | Central Management
   SI-8(2): Spam Protection | Automatic Updates
SI-9: INFORMATION INPUT RESTRICTIONS [WITHDRAWN FROM NIST 800-53 REV4]
SI-10: INPUT DATA VALIDATION
SI-11: ERROR HANDLING
SI-12: INFORMATION OUTPUT HANDLING & RETENTION
SI-13: PREDICTABLE FAILURE ANALYSIS
   CP-10(5): Information System Recovery & Reconstitution | Failover Capability
SI-14: NON-PERSISTENCE
SI-15: INFORMATION OUTPUT FILTERING
SI-16: MEMORY PROTECTION
SI-17: FAIL-SAFE PROCEDURES
 PRIVACY CONTROLS 160

AUTHORITY & PURPOSE (AP) 160
  AP-1: AUTHORITY TO COLLECT 160
  AP-2: PURPOSE SPECIFICATION 160

ACCOUNTABILITY, AUDIT & RISK MANAGEMENT (AR) 161
  AR-1: GOVERNANCE & PRIVACY PROGRAM 161
  AR-2: PRIVACY IMPACT & RISK ASSESSMENT 161
  AR-3: PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS 162
  AR-4: PRIVACY MONITORING & AUDITING 162
  AR-5: PRIVACY AWARENESS & TRAINING 162
  AR-6: PRIVACY REPORTING 162
  AR-7: PRIVACY-ENHANCED SYSTEM DESIGN & DEVELOPMENT 162
  AR-8: ACCOUNTING OF DISCLOSURES 163

DATA QUALITY & INTEGRITY (DI) 164
  DI-1: DATA QUALITY 164
  DI-2: DATA INTEGRITY 164

DATA MINIMIZATION & RETENTION (DM) 165
  DM-1: MINIMIZATION OF PERSONAL DATA (PD) 165
  DM-2: DATA RETENTION & DISPOSAL 165
  DM-3: MINIMIZATION OF PD USED IN TESTING, TRAINING & RESEARCH 166

INDIVIDUAL PARTICIPATION & REDRESS (IP) 168
  IP-1: CONSENT 168
  IP-2: INDIVIDUAL ACCESS 168
  IP-3: REDRESS 168
  IP-4: USER FEEDBACK MANAGEMENT 169

SECURITY (SE) 170
  SE-1: INVENTORY OF PERSONAL DATA (PD) 170
  SE-2: PRIVACY INCIDENT RESPONSE 170

TRANSPARENCY (TR) 171
  TR-1: PRIVACY NOTICE 171
  TR-2: SAFE HARBOR 171
  TR-3: DISSEMINATION OF PRIVACY PROGRAM INFORMATION 173

USE LIMITATION (UL) 174
  UL-1: INTERNAL USE 174
  UL-2: INFORMATION SHARING WITH THIRD PARTIES 174

GLOSSARY: ACRONYMS & DEFINITIONS 175
ACRONYMS 175
DEFINITIONS 175

KEY WORD INDEX 176

RECORD OF CHANGES 177

APPENDIX A - CYBERSECURITY POLICIES SUMMARY 178
POLICY STATEMENT 1: SECURITY ASSESSMENT & AUTHORIZATION (CA) 178
POLICY STATEMENT 2: PLANNING (PL) 178
POLICY STATEMENT 3: PROGRAM MANAGEMENT (PM) 179
POLICY STATEMENT 4: RISK ASSESSMENT (RA) 179
POLICY STATEMENT 5: SYSTEM & SERVICES ACQUISITION (SA) 179
POLICY STATEMENT 6: AWARENESS & TRAINING (AT) 179
POLICY STATEMENT 7: CONTINGENCY PLANNING (CP) 179
POLICY STATEMENT 8: INCIDENT RESPONSE (IR) 180
POLICY STATEMENT 9: MEDIA PROTECTION (MP) 180
POLICY STATEMENT 10: PERSONNEL SECURITY (PS) 180
POLICY STATEMENT 11: PHYSICAL & ENVIRONMENTAL PROTECTION (PE) 180
POLICY STATEMENT 12: ACCESS CONTROL (AC) 180
POLICY STATEMENT 13: AUDIT & ACCOUNTABILITY (AU) 181
POLICY STATEMENT 14: CONFIGURATION MANAGEMENT (CM) 181
POLICY STATEMENT 15: IDENTIFICATION & AUTHENTICATION (IA) 181
POLICY STATEMENT 16: MAINTENANCE (MA) 181
POLICY STATEMENT 17: SYSTEM & COMMUNICATION PROTECTION (SC) 181
POLICY STATEMENT 18: SYSTEM & INFORMATION INTEGRITY (SI) 182
POLICY STATEMENT 19: AUTHORITY & PURPOSE (AP) 182
POLICY STATEMENT 20: ACCOUNTABILITY, AUDIT & RISK MANAGEMENT (AR) 182
POLICY STATEMENT 21: DATA QUALITY & INTEGRITY (DI) 182
POLICY STATEMENT 22: DATA MINIMIZATION & RETENTION (DM) 182
POLICY STATEMENT 23: INDIVIDUAL PARTICIPATION & REDRESS (IP) 183
POLICY STATEMENT 24: SECURITY (SE) 183
POLICY STATEMENT 25: TRANSPARENCY (TR) 183
POLICY STATEMENT 26: USE LIMITATION (UL) 183
**INTRODUCTION**

The Written Information Security Program (WISP) provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at ACME Business Solutions, LLC (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with ACME data and/or systems. Therefore, it is the responsibility of VENDOR to be aware of and adhere to ACME’s cybersecurity requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure the confidentiality, availability and integrity of the data:

Commensurate with risk, cybersecurity and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:

- **Confidentiality** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **Integrity** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** – Availability addresses ensuring timely and reliable access to and use of information.
- **Safety** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

**PURPOSE**

The purpose of the Written Information Security Program (WISP) is to prescribe a comprehensive framework for:

- Creating a NIST-based Information Security Management System (ISMS);
- Protecting the confidentiality, integrity and availability of ACME data and systems;
- Protecting ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensuring the effectiveness of security controls over data and systems that support ACME’s operations;
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review and maintenance of minimum security controls required to protect ACME’s data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which ACME operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related standards, procedures and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure ACME users understand their day-to-day security responsibilities and the threats that could impact the company.
Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of ACME data.

**SCOPE & APPLICABILITY**

These policies, standards, procedures and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards, procedures and guidelines apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME data.

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions shall comply with the policies. ACME departments shall use these policies or may create a more restrictive policy, but none that are less restrictive, less comprehensive or less compliant than these policies.

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

ACME’s documented cybersecurity roles & responsibilities provides a detailed description of ACME user roles and responsibilities, in regards to cybersecurity.

ACME reserves the right to revoke, change or supplement these policies, standards, procedures and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management unless otherwise stated.

**POLICY OVERVIEW**

To ensure an acceptable level of Cybersecurity risk, ACME is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

ACME users are required to protect and ensure the Confidentiality, Integrity and Availability (CIA) of data and systems, regardless of how its data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

**VIOLATIONS**

Any ACME user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

**EXCEPTIONS**

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. Users are required to submit a request for an exception to a cybersecurity standard and receive approval for the exception, before any deviation from a standard can be implemented.

**UPDATES**

Updates to the Written Information Security Program (WISP) will be announced to employees via management updates or email announcements. Changes will be noted in the [Record of Changes](#) to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.
**KEY TERMINOLOGY**

In the realm of Cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the primary reference document that ACME uses to define common Cybersecurity terms.¹ Key terminology to be aware of includes:

**Asset Custodian:** A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended and that information regarding the equipment is properly documented.

**Cardholder Data Environment (CDE):** A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage or transmission. Adequate network segmentation, which isolates systems that store, process or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.

**Control:** A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

**Applicability:** A term describing the scope in which a control or standard is relevant and applicable.

**Control Objective:** A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align ACME with accepted due care requirements.

**Controlled Unclassified Information (CUI):** CUI is a broad range of sensitive data that is defined by the US National Archives on the CUI Registry website.²

**Data:** A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. *Annex 1: Data Classification & Handling Guidelines* provides guidance on data classification and handling restrictions.

**Data Owner:** A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.

**Encryption:** A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

**Guidelines:** A term describing recommended practices that are based on industry-recognized secure practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

**Cybersecurity:** A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity and Availability (CIA) of data.

**Least Privilege:** A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

**Personally Data (PD):** PD is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements:³

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or other government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

---


² US National Archives – CUI Registry - [https://www.archives.gov/cui](https://www.archives.gov/cui)

³ The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - [https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html](https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html) and Massachusetts 201 CMR 17.00“ Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 [http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf](http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf)
**POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE**

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 Diagram](image)

**CYBERSECURITY CONTROL OBJECTIVES**

ACME’s standards are organized into classes and families for ease of use in the control selection and specification process. There are four (4) general classes of security control objectives that align with FIPS 199. These classes are further broken down into twenty-six (26) families of security control objectives.

- **Management**
  - Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics.
  - Management controls also play an important role in policy enforcement, since these focus on the management of the cybersecurity program and the management of risk within ACME.

- **Operational**
  - Operational controls are primarily focused on resource the execution of the day-to-day cybersecurity program.
  - These controls generally focus on the means to control logical and physical access to information and to protect the security of supporting systems.

- **Technical**
  - Technical controls are primarily technical in nature. These controls, such as devices, processes, protocols and other measures, are used to protect the confidentiality, integrity and availability of the organization’s technology assets and data.
  - These are dependent upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations.

- **Privacy**

---

The focus is on controls that impact Personal Data (PD).
These dependent upon the proper functioning of the other classes of controls for their effectiveness and therefore require significant operational considerations.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. The table below summarizes the classes and families in the security control catalog and the associated family identifiers.

<table>
<thead>
<tr>
<th>FIPS 199 Focus</th>
<th>Family</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Security Assessment &amp; Authorization</td>
<td>CA</td>
</tr>
<tr>
<td>Management</td>
<td>Planning</td>
<td>PL</td>
</tr>
<tr>
<td>Management</td>
<td>Program Management</td>
<td>PM</td>
</tr>
<tr>
<td>Management</td>
<td>Risk Assessment</td>
<td>RA</td>
</tr>
<tr>
<td>Management</td>
<td>System &amp; Services Acquisition</td>
<td>SA</td>
</tr>
<tr>
<td>Operational</td>
<td>Awareness &amp; Training</td>
<td>AT</td>
</tr>
<tr>
<td>Operational</td>
<td>Contingency Planning</td>
<td>CP</td>
</tr>
<tr>
<td>Operational</td>
<td>Incident Response</td>
<td>IR</td>
</tr>
<tr>
<td>Operational</td>
<td>Media Protection</td>
<td>MP</td>
</tr>
<tr>
<td>Operational</td>
<td>Personnel Security</td>
<td>PS</td>
</tr>
<tr>
<td>Operational</td>
<td>Physical &amp; Environmental Protection</td>
<td>PE</td>
</tr>
<tr>
<td>Technical</td>
<td>Access Control</td>
<td>AC</td>
</tr>
<tr>
<td>Technical</td>
<td>Audit &amp; Accountability</td>
<td>AU</td>
</tr>
<tr>
<td>Technical</td>
<td>Configuration Management</td>
<td>CM</td>
</tr>
<tr>
<td>Technical</td>
<td>Identification &amp; Authentication</td>
<td>IA</td>
</tr>
<tr>
<td>Technical</td>
<td>Maintenance</td>
<td>MA</td>
</tr>
<tr>
<td>Technical</td>
<td>System &amp; Communications Protection</td>
<td>SC</td>
</tr>
<tr>
<td>Technical</td>
<td>System &amp; Information Integrity</td>
<td>SI</td>
</tr>
<tr>
<td>Privacy</td>
<td>Authority &amp; Purpose</td>
<td>AP</td>
</tr>
<tr>
<td>Privacy</td>
<td>Accountability, Audit &amp; Risk Management</td>
<td>AR</td>
</tr>
<tr>
<td>Privacy</td>
<td>Data Quality &amp; Integrity</td>
<td>DI</td>
</tr>
<tr>
<td>Privacy</td>
<td>Data Minimization &amp; Retention</td>
<td>DM</td>
</tr>
<tr>
<td>Privacy</td>
<td>Individual Participation &amp; Redress</td>
<td>IP</td>
</tr>
<tr>
<td>Privacy</td>
<td>Security</td>
<td>SE</td>
</tr>
<tr>
<td>Privacy</td>
<td>Transparency</td>
<td>TR</td>
</tr>
<tr>
<td>Privacy</td>
<td>Use Limitation</td>
<td>UL</td>
</tr>
</tbody>
</table>

*Figure 2: NIST SP 800-53 Control Objectives Families & Identifiers*
An Information Security Management System (ISMS) focuses on Cybersecurity management and IT-related risks. The governing principle behind ACME’s ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with ISO/IEC 27001, ACME’s ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA) or Deming Cycle, approach:

- **Plan**: This phase involves designing the ISMS, assessing IT-related risks and selecting appropriate controls.
- **Do**: This phase involves implementing and operating the appropriate security controls.
- **Check**: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- **Act**: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

**Cybersecurity Considerations For Protecting Systems**

ACME’s cybersecurity considerations for protecting systems are based on the following criteria:

- The criticality of the system / application / process; and
- The sensitivity of the data that is stored, processed and/or transmitted by that system / application / process.
**MANAGEMENT CONTROLS**

Management controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity topics. These cybersecurity controls address broader Information Security Management System (ISMS)-level governance of the security program that impact operational, technical and privacy controls.

**PROGRAM MANAGEMENT (PM)**

**Cybersecurity Program Management Policy:** ACME shall implement Cybersecurity program management controls to provide a foundation for ACME’s cybersecurity Management System (ISMS).

**Management Intent:** The purpose of the Program Management (PM) policy is for ACME to specify the development, implementation, assessment, authorization and monitoring of the Cybersecurity program management. The successful implementation of security controls for organizational systems depends on the successful implementation of the organization’s program management controls. The Cybersecurity Program Management (PM) controls are essential for managing the Cybersecurity program.

**Supporting Documentation:** Program Management (PM) control objectives, standards and guidelines directly support this policy.

**PM-1: INFORMATION SECURITY PROGRAM PLAN**

**Control Objective:** The organization:

- Develops and disseminates organization-wide cybersecurity standards that:
  - Provides an overview of the requirements for the cybersecurity program and a description of the controls in place or planned, for meeting those requirements;
  - Provides sufficient information about controls to enable an implementation that is unambiguously compliant with the intent of the plan;
  - Includes roles, responsibilities, management commitment and compliance;
  - Is approved by senior management with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image and reputation), organizational assets, individuals and other organizations;
  - Reviews standards for applicability; and
  - Revises standards to address organizational changes and problems identified during implementation or security assessments.

**Standard:** ACME’s cybersecurity policies and standards shall be represented in a single document, the Written Information Security Program (WISP) that shall be:

(a) Endorsed by executive management;
(b) Reviewed and updated at least annually; and
(c) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

**Supplemental Guidance:** The security plans for individual systems and the organization-wide cybersecurity program plan together, provide complete coverage for all security controls employed within the organization.

**PM-2: SENIOR INFORMATION SECURITY OFFICER**

**Control Objective:** The organization appoints an individual assigned with the mission and resources to coordinate, develop, implement and maintain an organization-wide cybersecurity program.

**Standard:** The authority and responsibility for managing the cybersecurity program are delegated to ACME’s Information Security Officer (ISO) and he/she is required to perform or delegate the following cybersecurity management responsibilities:

(a) Establish, document and distribute security policies and procedures;

---

5 HIPAA 164.308(a)(1)(I) & 164.316(a)-(b) | GLBA Sec 6801(b)(a) | PCI DSS 12.1 & 12.1.1 | MA201CMR17 17.03(1), 17.04 & 17.03(2)(b)(b) | NIST CSF ID.GV-1 & ID.GV-2 | DFARS 252.204-7008 | NY DFS 500.02 & 500.03
6 HIPAA 164.308(a)(2) | GLBA Safeguards Rule | PCI DSS 12.5-12.5.5 | MA201CMR17 17.03(2)(a) | OR646A.622(2)(d)(A)(i) | NIST CSF ID.AM-6 & ID.GV-2 | NY DFS 500.04
(b) Monitor and analyze security alerts and information;
(c) Distribute and escalate security alerts to appropriate personnel;
(d) Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
(e) Administer user accounts, including additions, deletions and modifications; and
(f) Monitor and control all access to data.

Supplemental Guidance: None

**PM-3: INFORMATION SECURITY RESOURCES**

**Control Objective:** The organization addresses all capital planning and investment requests, including the resources needed to implement the cybersecurity program and documents all exceptions to this requirement.

**Standard:** The Information Security Officer (ISO) and his/her designated representatives are responsible for managing and providing oversight for the cybersecurity-related aspects of the planning and service / tool selection process.

**Supplemental Guidance:** None

**PM-4: PLAN OF ACTION & MILESTONES (POA&M) PROCESS (VULNERABILITY REMEDIATION)**

**Control Objective:** The organization implements a process for ensuring that vulnerabilities are properly identified, documents remediation actions and tracks vulnerabilities to mitigate risk to operations, assets, individuals and other organizations. 7

**Standard:** ACME is required to use a Plan of Action & Milestones (POA&M) or some other company-approved method, as a key tool in documenting identified weaknesses, their status and remediation steps.

**Supplemental Guidance:** POA&M-related issues shall be based on the findings from security control assessments, security impact analyses and continuous monitoring activities.

**PM-5: INFORMATION SYSTEM INVENTORY**

**Control Objective:** The organization develops and maintains an inventory of its systems. 8

**Standard:** ACME is required to maintain an inventory of its systems that includes, but is not limited to:
(a) A list of all such devices and personnel with access;
(b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding, and/or inventorying of devices);
(c) List of company-approved products; and
(d) Update the inventory at necessary.

**Supplemental Guidance:** It is also possible that the owner and custodian of the hardware, software and data are the same, but this needs to be identified and documented.

**PM-6: INFORMATION SECURITY MEASURES OF PERFORMANCE**

**Control Objective:** The organization develops, monitors and reports on the results of cybersecurity measures of performance. 9

**Standard:** The Information Security Officer (ISO) shall develop measures of performance or outcome-based metrics, to measure the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program.

**Supplemental Guidance:** Measures of performance are outcome-based metrics used by ACME to measure the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program.

---

7 MA201CMR17 17.03(2)(j(j | OR646A.622(2)(d)(ii)(ii) | NIST CSF ID.RA-6
8 PCI DSS 12.3.3, 12.3.4 & 12.3.7 | NIST CSF ID.AM-1 & ID.AM-2
9 HIPAA 164.308(a)(8) | SOX Sec 404 | MA201CMR17 17.03(2)(j) | OR646A.622(2)(d)(i)(vi) & OR646A.622(2)(d)(ii)(iii) | NIST CSF ID.AM-2 & PR.IP-7
OPERATIONAL CONTROLS

Operational Controls are primarily focused on resource protection. Operational Controls generally focus on the means to control access to information and to protect the availability of that information. Management and Technical controls depend on proper Operational Controls being in place. A Management Control allowing only authorized personnel access to the data center does little good without some kind of Operational Control that addresses access.

AWARENESS & TRAINING (AT)

Awareness & Training Policy: ACME shall ensure that users are made aware of the security risks associated with their roles and that users understand the applicable laws, policies, standards and procedures related to the security of systems and data.

Management Intent: The purpose of the Awareness & Training (AT) policy is to provide guidance for broad security awareness and security training for ACME users.

Supporting Documentation: Awareness & Training (AT) control objectives, standards and guidelines directly support this policy.

AT-1: SECURITY AWARENESS & TRAINING POLICY & PROCEDURES

Control Objective: The organization develops, disseminates, reviews & updates: 50

- A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
- Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Standard: ACME is required to document organization-wide security awareness and training controls that, at a minimum, include:

(a) A formal, documented security awareness and training policy; and
(b) Processes to facilitate the implementation of the security awareness and training policy, standards and procedures.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable laws, regulations, policies, standards and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

The security awareness and training program should include, at a minimum, the following components:

- Training goals;
- Target audience(s);
- Learning objectives;
- Deployment methods;
- Evaluation method to determine training effectiveness;
- Frequency;
- Duration;
- Deliverables or handouts; and
- Attendance tracking

AT-2: SECURITY AWARENESS TRAINING

Control Objective: The organization provides basic security awareness training to all system users (including managers, senior executives and contractors) as part of initial training for new users, when required by system changes and thereafter as required. 51

Standard: ACME’s cybersecurity personnel are responsible for developing and implementing a formal security awareness program to make all ACME users aware of the importance of cybersecurity.

50 NY DFS 500.14
51 HIPAA 164.308(a)(5)(i) & 164.308(a)(5)(ii)(A) | PCI DSS 12.6 | MA201CMR17 17.04(8) & 17.03(2)(b)(a) | NIST CSF PR.AT-1 | NY DFS 500.14
Supplemental Guidance: Organizations generally determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for cybersecurity and user actions to maintain security and to respond to suspected security incidents.

**AT-2(2): SECURITY AWARENESS TRAINING | INSIDER THREAT**

Control Objective: The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Standard: ACME’s cybersecurity personnel are required to implement security awareness training that includes how to identify and report potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include concerning behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow colleagues, workplace violence and other serious violations of organizational policies, procedures, directives, rules, and/or practices.

**AT-3: ROLE-BASED SECURITY TRAINING**

Control Objective: The organization provides role-based security-related training:

- Before authorizing access to the system or performing assigned duties;
- When required by system changes; and
- Annually thereafter.

Standard: For cybersecurity training:

(a) Human Resources (HR) and users’ direct management shall provide initial security training to personnel upon hire;
(b) ACME’s cybersecurity personnel are required to provide training at least annually, thereafter;
(c) ACME’s management is required to ensure that every user accessing a system that processes, stores or transmits sensitive information is formally trained in handling procedures for all of the relevant types of sensitive information; and
(d) Incorporate relevant security training to all employees and/or contractors that are involved in the deployment of cybersecurity-oriented solutions to maintain professional competency in their assigned role and responsibility.

Supplemental Guidance: Initial orientation and ongoing security training should include the following topics:

- Cybersecurity basics
- Company cybersecurity policies
- Email policy
- Acceptable usage policy
- Data classification & handling
- Malicious software & spam
- Offsite security / security at home
- Wireless security
- Third party security (outsourced vendors)
- Visitor security procedures
- Incident response procedures
- Business continuity roles and procedures

Methods can vary depending on the role of the personnel and their level of access to sensitive data. For end-user training:

- All users must sign an acknowledgment form stating they have read and understood ACME’s requirements regarding cybersecurity policies, standards, procedures and guidelines prior to having access to ACME systems or data.
- All new users must attend a security awareness training class within thirty (30) days of being granted access to any system;
- All users shall undergo at least one (1) hour of security awareness training annually.
- All users must be provided with sufficient training and supporting reference materials to allow them to properly protect ACME’s systems and data; and
- ACME’s management must develop and maintain a communications process to be able to communicate new Cybersecurity program information, such as an informational security bulletin or email about security items of interest.

---

52 PCI DSS 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.9, 11.6, 12.6, 12.6.1, 12.6.2, 12.8.3 & 12.8.5, 12.10.4 | MA201CMR17 17.04(8) | OR646A.622(2)(d)(A)(iv) | NIST CSF PR-AT-2, PR-AT-4 & PR-AT-5 | NY DFS 500.10 & 500.14
**INCIDENT RESPONSE (IR)**

**Incident Response Policy:** ACME shall establish an actionable Cybersecurity incident handling capability that includes adequate preparation, detection, analysis, containment, recovery and reporting activities.

**Management Intent:** The purpose of Incident Response (IR) policy is to establish a protocol to guide ACME’s response to a cybersecurity incident.

**Supporting Documentation:** Incident Response (IR) control objectives, standards and guidelines directly support this policy.

**IR-1: INCIDENT RESPONSE POLICY & PROCEDURES**

**Control Objective:** The organization develops, disseminates, reviews & updates:

- A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and
- Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

**Standard:** ACME is required to document organization-wide incident response controls that, at a minimum, include:

(a) A formal, documented incident response policy; and
(b) Processes to facilitate the implementation of the incident response policy, standards and procedures.

**Supplemental Guidance:** This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable laws, regulations, policies, standards and guidance. Security program policies and procedures at the organization level may make the need for systemspecific policies and procedures unnecessary. The policy can be included as part of the general cybersecurity policy for organizations. The procedures can be established for the security program in general and for particular systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

**IR-2: INCIDENT RESPONSE TRAINING**

**Control Objective:** The organization:

- Trains personnel in their incident response roles and responsibilities with respect to systems; and
- Provides refresher training.

**Standard:** ACME’s Information Security Officer (ISO) is required to implement role-based incident response training that:

(a) Trains personnel in their incident response roles and responsibilities; and
(b) Provides refresher training.

**Supplemental Guidance:** Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

**IR-3: INCIDENT RESPONSE TESTING**

**Control Objective:** The organization tests and/or exercises the incident response capability for systems using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.

**Standard:** ACME management and IT staff are required to perform annual tests and/or exercises of its incident response capability to formally determine incident response effectiveness and make corrections, based on any deficiencies.
Supplemental Guidance: Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walkthrough or tabletop exercises, simulations (parallel/full interrupt) and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets and individuals due to incident response.

**IR-3(2): INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS**

**Control Objective:** The organization coordinates incident response testing with organizational elements responsible for related plans.

**Standard:** Data/process owners must ensure coordinated incident response testing is conducted with appropriate personnel responsible for related plans.

**Supplemental Guidance:** Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans and Occupant Emergency Plans.

**IR-4: INCIDENT HANDLING**

**Control Objective:** The organization:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training and testing/exercises and implements the resulting changes accordingly.

**Standard:** ACME management and IT staff are required:

(a) Identify the severity and classification of incidents; and
(b) Define appropriate actions to take in response to ensure the continuation of business functions.

**Supplemental Guidance:** Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices and the risk executive (function).

**IR-4(1): INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES**

**Control Objective:** The organization employs automated mechanisms to support the incident handling process.

**Standard:** Where technically feasible and a business justification exists, ACME shall employ automated mechanisms to support the incident handling process.

**Supplemental Guidance:** Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

**IR-5: INCIDENT MONITORING**

**Control Objective:** The organization tracks and documents system security incidents.

**Standard:** ACME management and IT staff are responsible for managing and documenting security incidents.

---

65 PCI DSS 12.5.3 | NIST CSF DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.MI-1, RS.MI-2, RS.RP-1, RC.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3 | NY DFS 500.16

66 PCI DSS 12.5.2 | NIST CSF DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4
Supplemental Guidance: Documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident and other pertinent information necessary for forensics, evaluating incident details, trends and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring and user/administrator reports.

**IR-6: INCIDENT REPORTING**

**Control Objective:** The organization:

- Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
- Reports security incident information to designated authorities.

**Standard:** ACME’s Cybersecurity Incident Response Program (CIRP) addresses incident reporting, both internally and externally:

(a) Users are responsible for reporting system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to ACME’s cybersecurity personnel;
(b) Upon discovery of an incident that affects Personal Data (PD), ACME’s Data Protection Officer (DPO) must be notified; and
(c) Upon discovery of a cyber incident that affects a Covered Contractor Information System (CCIS) or the Covered Defense Information (CDI) residing therein or that affects ACME’s ability to perform the requirements of the contract that are designated as operationally critical support, ACME shall:
   i. Conduct a review of evidence of compromise of CDI, including, but not limited to, identifying compromised computers, servers, specific data and user accounts.
      1. This review shall also include analyzing CCIS(s) that were part of the cyber incident, as well as other information systems on ACME’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information or that affect ACME’s ability to provide operationally critical support; and
   ii. The cyber incident report shall be treated as information created by or for Department of Defense (DoD) and shall include, at a minimum, the required elements at [http://dibnet.dod.mil](http://dibnet.dod.mil);
   iii. If applicable, submit identified and contained malicious software in accordance with instructions provided by the DoD Contracting Officer;
   iv. Preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least ninety (90) days from the submission of the cyber incident report to allow DoD to request the media or decline interest; and
   v. Upon request by DoD, provide DoD with:
      1. Access to additional information or equipment that is necessary to conduct a forensic analysis; and
      2. All of the damage assessment information gathered.

Supplemental Guidance: If a breach occurs, breach notification procedures should occur without unreasonable delay, except:

- When a law enforcement agency has determined that notification will impede a criminal investigation; or
- In order to discover the complete scope of the breach and restore the integrity of the system.

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports and the designated reporting authorities reflect applicable laws, policies, regulations, standards and guidance.

In terms of incident reporting, the definition of a security breach is when an individual’s unencrypted Personal Data (PD) is reasonably believed to have been acquired by an unauthorized person or process. Good faith acquisition of PD by an authorized user or authorized agent for ACME purposes does not constitute a security breach, provided that the PD is not used or subject to further unauthorized disclosure.

**IR-6(1): INCIDENT REPORTING | AUTOMATED REPORTING**

**Control Objective:** The organization employs automated mechanisms to assist in the reporting of security incidents.
SUPPLEMENTAL DOCUMENTATION

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

ANNEXES, TEMPLATES & REFERENCES

Version 2020.1
<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
</table>

Annexes

<table>
<thead>
<tr>
<th>Annex</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Classification &amp; Handling Guidelines</td>
</tr>
<tr>
<td>2</td>
<td>Data Classification Examples</td>
</tr>
<tr>
<td>3</td>
<td>Data Retention Periods</td>
</tr>
<tr>
<td>4</td>
<td>Baseline Security Categorization Guidelines</td>
</tr>
<tr>
<td>5</td>
<td>Rules of Behavior (Acceptable &amp; Unacceptable Use)</td>
</tr>
<tr>
<td>6</td>
<td>Guidelines for Personal Use of Organizational IT Resources</td>
</tr>
<tr>
<td>7</td>
<td>Risk Management Framework (RMF)</td>
</tr>
<tr>
<td>8</td>
<td>System Hardening</td>
</tr>
</tbody>
</table>

Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Management Directive (Policy Authorization)</td>
</tr>
<tr>
<td>2</td>
<td>User Acknowledgement Form</td>
</tr>
<tr>
<td>3</td>
<td>User Equipment Receipt of Issue</td>
</tr>
<tr>
<td>4</td>
<td>Service Provider Non-Disclosure Agreement (NDA)</td>
</tr>
<tr>
<td>5</td>
<td>Incident Response Plan (IRP)</td>
</tr>
<tr>
<td>6</td>
<td>Incident Response Form</td>
</tr>
<tr>
<td>7</td>
<td>Appointment Orders (Information Security Officer)</td>
</tr>
<tr>
<td>8</td>
<td>Privileged User Account Request Form</td>
</tr>
<tr>
<td>9</td>
<td>Change Management Request Form</td>
</tr>
<tr>
<td>10</td>
<td>Change Control Board (CCB) Meeting Minutes</td>
</tr>
<tr>
<td>11</td>
<td>Plan of Action &amp; Milestones (POA&amp;M) / Risk Register</td>
</tr>
<tr>
<td>12</td>
<td>Ports, Protocols &amp; Services (PPS)</td>
</tr>
<tr>
<td>13</td>
<td>Business Impact Analysis (BIA)</td>
</tr>
<tr>
<td>14</td>
<td>Disaster Recovery Plan (DRP) &amp; Business Continuity Plan (BCP)</td>
</tr>
<tr>
<td>15</td>
<td>Privacy Impact Assessment (PIA)</td>
</tr>
</tbody>
</table>

References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WISP Exception Request Process</td>
</tr>
<tr>
<td>2</td>
<td>Electronic Discovery (eDiscovery) Guidelines</td>
</tr>
<tr>
<td>3</td>
<td>Types of Security Controls</td>
</tr>
<tr>
<td>4</td>
<td>Information Security Management System (ISMS)</td>
</tr>
</tbody>
</table>
ANNEXES

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION
Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

<table>
<thead>
<tr>
<th>CLASSIFICATION</th>
<th>DATA CLASSIFICATION DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RESTRICTED</strong></td>
<td>Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.</td>
</tr>
<tr>
<td>Potential Impact of Loss</td>
<td>• <strong>SIGNIFICANT DAMAGE</strong> would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME.</td>
</tr>
<tr>
<td></td>
<td>• Impact could include negatively affecting ACME’s competitive position, violating regulatory requirements, damaging the company’s reputation, violating contractual requirements, and posing an identity theft risk.</td>
</tr>
<tr>
<td><strong>CONFIDENTIAL</strong></td>
<td>Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by ACME.</td>
</tr>
<tr>
<td>Potential Impact of Loss</td>
<td>• <strong>MODERATE DAMAGE</strong> would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME.</td>
</tr>
<tr>
<td></td>
<td>• Impact could include negatively affecting ACME’s competitive position, damaging the company’s reputation, violating contractual requirements, and exposing the geographic location of individuals.</td>
</tr>
<tr>
<td><strong>INTERNAL USE</strong></td>
<td>Internal Use information is information originated or owned by ACME, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company’s business interests.</td>
</tr>
<tr>
<td>Potential Impact of Loss</td>
<td>• <strong>MINIMAL or NO DAMAGE</strong> would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME.</td>
</tr>
<tr>
<td></td>
<td>• Impact could include damaging the company’s reputation and violating contractual requirements.</td>
</tr>
<tr>
<td><strong>PUBLIC</strong></td>
<td>Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.</td>
</tr>
<tr>
<td>Potential Impact of Loss</td>
<td>• <strong>NO DAMAGE</strong> would occur if Public information were to become available to parties either internal or external to ACME.</td>
</tr>
<tr>
<td></td>
<td>• Impact would not be damaging or a risk to business operations.</td>
</tr>
</tbody>
</table>
**LABELING**

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed.** Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.

- **Displayed.** Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

### GENERAL ASSUMPTIONS

- Any information created or received by ACME employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

### PERSONAL DATA (PD)

PD is any information about an individual maintained by ACME including any information that:

- Can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD. Examples of PD include, but are not limited to:

- **Name**
  - Full name;
  - Maiden name;
  - Mother’s maiden name; and
  - Alias(es);
- **Personal Identification Numbers**
  - Social Security Number (SSN);
  - Passport number;
  - Driver’s license number;
  - Taxpayer Identification Number (TIN), and
  - Financial account or credit card number;
- **Address Information**
  - Home address; and
  - Personal email address;
- **Personal Characteristics**
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting,
# Data Handling Guidelines

<table>
<thead>
<tr>
<th>Handling Controls</th>
<th>Restricted</th>
<th>Confidential</th>
<th>Internal Use</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-Disclosure Agreement (NDA)</strong></td>
<td>• NDA is required prior to access by non-ACME employees.</td>
<td>• NDA is recommended prior to access by non-ACME employees.</td>
<td>No NDA requirements</td>
<td>No NDA requirements</td>
</tr>
<tr>
<td><strong>Internal Network Transmission</strong></td>
<td>• Encryption is required • Instant Messaging is prohibited • FTP is prohibited</td>
<td>• Encryption is required • Instant Messaging is prohibited • FTP is prohibited</td>
<td>No special requirements</td>
<td>No special requirements</td>
</tr>
<tr>
<td>(wired &amp; wireless)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>External Network Transmission</strong></td>
<td>• Encryption is required • Instant Messaging is prohibited • FTP is prohibited • Remote access should be used only when necessary and only with VPN and two-factor authentication</td>
<td>• Encryption is required • Instant Messaging is prohibited • FTP is prohibited • Remote access should be used only when necessary and only with VPN and two-factor authentication</td>
<td>No special requirements</td>
<td>No special requirements</td>
</tr>
<tr>
<td>(wired &amp; wireless)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data At Rest</strong></td>
<td>• Encryption is required • Logical access controls are required to limit unauthorized use • Physical access restricted to specific individuals</td>
<td>• Encryption is required • Logical access controls are required to limit unauthorized use • Physical access restricted to specific individuals</td>
<td>• Encryption is required • Logical access controls are required to limit unauthorized use • Physical access restricted to specific individuals</td>
<td>• Logical access controls are required to limit unauthorized use • Physical access restricted to specific groups</td>
</tr>
<tr>
<td>(file servers, databases, archives, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mobile Devices</strong></td>
<td>• Encryption is required • Remote wipe must be enabled, if possible</td>
<td>• Encryption is required • Remote wipe must be enabled, if possible</td>
<td>• Encryption is recommended • Remote wipe should be enabled, if possible</td>
<td>No special requirements</td>
</tr>
<tr>
<td>(iPhone, iPad, MP3 player, USB drive, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>• Encryption is required • Do not forward</td>
<td>• Encryption is required • Do not forward</td>
<td>• Encryption is recommended</td>
<td>No special requirements</td>
</tr>
<tr>
<td>(with and without attachments)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical Mail</strong></td>
<td>• Mark “Open by Addressee Only” • Use “Certified Mail” and sealed, tamper-resistant envelopes for external mailings • Delivery confirmation is required • Hand deliver internally</td>
<td>• Mark “Open by Addressee Only” • Use “Certified Mail” and sealed, tamper-resistant envelopes for external mailings • Delivery confirmation is required • Hand delivering is recommended over interoffice mail</td>
<td>Mail with company interoffice mail • US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings</td>
<td>No special requirements</td>
</tr>
<tr>
<td><strong>Printer</strong></td>
<td>• Verify destination printer • Attend printer while printing</td>
<td>• Verify destination printer • Attend printer while printing</td>
<td>• Verify destination printer • Retrieve printed material without delay</td>
<td>No special requirements</td>
</tr>
</tbody>
</table>
ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

**IMPORTANT:** You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Sensitive Data Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client or Employee Personal</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>Social Security Number (SSN)</td>
</tr>
<tr>
<td></td>
<td>Employer Identification Number (EIN)</td>
</tr>
<tr>
<td></td>
<td>Driver’s License (DL) Number</td>
</tr>
<tr>
<td></td>
<td>Financial Account Number</td>
</tr>
<tr>
<td></td>
<td>Payment Card Number (credit or debit)</td>
</tr>
<tr>
<td></td>
<td>Government-Issued Identification (e.g., passport, permanent resident card, etc.)</td>
</tr>
<tr>
<td></td>
<td>Controlled Unclassified Information (CUI)</td>
</tr>
<tr>
<td></td>
<td>Birth Date</td>
</tr>
<tr>
<td></td>
<td>First &amp; Last Name</td>
</tr>
<tr>
<td></td>
<td>Age</td>
</tr>
<tr>
<td></td>
<td>Phone and/or Fax Number</td>
</tr>
<tr>
<td></td>
<td>Home Address</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
</tr>
<tr>
<td></td>
<td>Ethnicity</td>
</tr>
<tr>
<td></td>
<td>Email Address</td>
</tr>
<tr>
<td>Employee-Related Data</td>
<td>Compensation &amp; Benefits Data</td>
</tr>
<tr>
<td></td>
<td>Medical Data</td>
</tr>
<tr>
<td></td>
<td>Workers Compensation Claim Data</td>
</tr>
<tr>
<td></td>
<td>Education Data</td>
</tr>
<tr>
<td></td>
<td>Dependent or Beneficiary Data</td>
</tr>
<tr>
<td>Sales &amp; Marketing Data</td>
<td>Business Plan (including marketing strategy)</td>
</tr>
<tr>
<td></td>
<td>Financial Data Related to Revenue Generation</td>
</tr>
<tr>
<td></td>
<td>Marketing Promotions Development</td>
</tr>
<tr>
<td></td>
<td>Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)</td>
</tr>
<tr>
<td></td>
<td>News Releases</td>
</tr>
<tr>
<td>Networking &amp; Infrastructure Data</td>
<td>Username &amp; Password Pairs</td>
</tr>
<tr>
<td></td>
<td>Public Key Infrastructure (PKI) Cryptographic Keys (public &amp; private)</td>
</tr>
<tr>
<td></td>
<td>Hardware or Software Tokens (multifactor authentication)</td>
</tr>
<tr>
<td></td>
<td>System Configuration Settings</td>
</tr>
<tr>
<td></td>
<td>Regulatry Compliance Data</td>
</tr>
<tr>
<td></td>
<td>Internal IP Addresses</td>
</tr>
<tr>
<td></td>
<td>Privileged Account Usernames</td>
</tr>
<tr>
<td></td>
<td>Service Provider Account Numbers</td>
</tr>
<tr>
<td>Strategic Financial Data</td>
<td>Corporate Tax Return Information</td>
</tr>
<tr>
<td></td>
<td>Legal Billings</td>
</tr>
<tr>
<td></td>
<td>Budget-Related Data</td>
</tr>
<tr>
<td></td>
<td>Unannounced Merger and Acquisition Information</td>
</tr>
<tr>
<td></td>
<td>Trade Secrets (e.g., design diagrams, competitive information, etc.)</td>
</tr>
<tr>
<td>Operating Financial Data</td>
<td>Electronic Payment Information (Wire Payment / ACH)</td>
</tr>
<tr>
<td></td>
<td>Paychecks</td>
</tr>
<tr>
<td></td>
<td>Incentives or Bonuses (amounts or percentages)</td>
</tr>
<tr>
<td></td>
<td>Stock Dividend Information</td>
</tr>
<tr>
<td></td>
<td>Bank Account Information</td>
</tr>
</tbody>
</table>
The following schedule highlights suggested retention periods* for some of the major categories of data:
* Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TYPE OF RECORD</th>
<th>RETENTION PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Records</td>
<td>Amendments</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Annual Reports</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Articles of Incorporation</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Board of Directors (elections, minutes, committees, etc.)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Bylaws</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Capital stock &amp; bond records</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Charter</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Contracts &amp; agreements</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Copyrights</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Correspondence (General)</td>
<td>5 years</td>
</tr>
<tr>
<td></td>
<td>Correspondence (Legal)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Partnership agreement</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Patents</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Service marks</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Stock transfers</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Trademarks</td>
<td>Permanent</td>
</tr>
<tr>
<td>Financial Records</td>
<td>Audit report (external)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Audit report (internal)</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Balance sheets</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Bank deposit slips, reconciliations &amp; statements</td>
<td>7 years</td>
</tr>
<tr>
<td></td>
<td>Bills of lading</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Budgets</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Cash disbursement &amp; receipt record</td>
<td>7 years</td>
</tr>
<tr>
<td></td>
<td>Checks (canceled)</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Credit memos</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Depreciation schedule</td>
<td>7 years</td>
</tr>
<tr>
<td></td>
<td>Dividend register &amp; canceled dividend checks</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Employee expense reports</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Employee payroll records (W-2, W-4, annual earnings records, etc.)</td>
<td>7 years</td>
</tr>
<tr>
<td></td>
<td>Financial statements (annual)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Freight bills</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>General ledger</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Internal reports (work orders, sales reports, production reports)</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Inventory lists</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Investments (sales &amp; purchases)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Profit / Loss statements</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Purchase and sales contracts</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Purchase order</td>
<td>3 years</td>
</tr>
<tr>
<td></td>
<td>Subsidiary ledgers (accounts receivable, accounts payable, etc.)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Tax returns</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Vendor Invoices</td>
<td>7 years</td>
</tr>
<tr>
<td></td>
<td>Worthless securities</td>
<td>7 years</td>
</tr>
</tbody>
</table>
Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. This basis is called an Assurance Level (AL).

**DATA SENSITIVITY**
This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process.

**SAFETY & CRITICALITY**
The Safety & Criticality (SC) rating reflects two aspects of the “importance” of the asset or process:
- On one hand, SC simply represents the importance of the asset relative to the achievement of the company’s goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to ACME, its clients, its partners, or the general public.

The three (3) SC ratings are:
- **SC-1: Mission Critical.** This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of ACME:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on ACME’s mission.
    - Cannot go down without having a significant impact on ACME’s mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - Requires the most stringent protection measures that exceed leading practices to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- **SC-2: Business Critical.** This category involves systems, services and data that are determined to be important to the support of ACME’s business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on ACME’s mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - Requires protection measures equal to or beyond leading practices to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- **SC-3: Non-Critical.** This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on ACME’s mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - Requires protection measures that are commensurate with leading practices to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.
Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the “level of effort” that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

<table>
<thead>
<tr>
<th>Asset Categorization Matrix</th>
<th>Data Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RESTRICTED</td>
</tr>
<tr>
<td>SC-1 Mission Critical</td>
<td>Enhanced</td>
</tr>
<tr>
<td>SC-2 Business Critical</td>
<td>Enhanced</td>
</tr>
<tr>
<td>SC-3 Non-Critical</td>
<td>Enhanced</td>
</tr>
</tbody>
</table>

Figure 1: Asset Categorization Risk Matrix

**BASIC ASSURANCE REQUIREMENTS**
- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

**ENHANCED ASSURANCE REQUIREMENTS**
- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to ACME.
ACME maintains a cybersecurity risk management program to evaluate threats and vulnerabilities in order to assure the creation of appropriate remediation plans.

**RISK MANAGEMENT OVERVIEW**

There is sometimes conflict between cybersecurity and other general system/software engineering principles. Cybersecurity can sometimes be construed as interfering with "ease of use" where installing security countermeasures take more effort than a "trivial" installation that works, but is insecure. Often, this apparent conflict can be resolved by re-thinking the problem and it is generally possible to make a secure system also easy to use. Based on the value owners place on their assets, it is a necessity to impose countermeasures to mitigate any risks posed by specific threats.

**RISK MANAGEMENT FRAMEWORK (RMF)**

Risk management requires finding security equilibrium between vulnerabilities and acceptable security controls. This equilibrium can be thought of as acceptable risk – it changes as vulnerabilities and controls change. From a systems perspective, the components used to determine acceptable risk cover the entire Defense-in-Depth (DiD) breadth. If one component is weakened, another component must be strengthened to maintain the same level of security assurance. Risk management activities can be applied to both new and legacy systems.
**TEMPLATE 5: INCIDENT RESPONSE PLAN (IRP)**

By the very nature of every incident being somewhat different, the guidelines provided in this Incident Response Plan (IRP) do not comprise an exhaustive set of incident handling procedures. These guidelines document basic information about responding to incidents that can be used regardless of hardware platform or operating system. This plan describes the stages of incident identification and handling, with the focus on preparation and follow-up, including reporting guidelines and requirements.

**PLAN OBJECTIVES**
The objective of Incident Response Plan (IRP) is to:
- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;
- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of financial impact and loss of image;
- Update company policies, procedures, standards and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

**INCIDENT DISCOVERY**

<table>
<thead>
<tr>
<th>Malicious Actions</th>
<th>Possible Indications of an Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Denial of Service (DoS) Examples</strong></td>
<td>You might be experiencing a DoS if you see...</td>
</tr>
</tbody>
</table>
| Network-based DoS against a particular host | • User reports of system unavailability  
• Unexplained connection losses  
• Network intrusion detection alerts  
• Host intrusion detection alerts (until the host is overwhelmed)  
• Increased network bandwidth utilization  
• Large number of connections to a single host  
• Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host)  
• Firewall and router log entries  
• Packets with unusual source addresses |
| Network-based DoS against a network | • User reports of system and network unavailability  
• Unexplained connection losses  
• Network intrusion detection alerts  
• Increased network bandwidth utilization  
• Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network)  
• Firewall and router log entries  
• Packets with unusual source addresses  
• Packets with nonexistent destination addresses |
| DoS against the operating system of a particular host | • User reports of system and application unavailability  
• Network and host intrusion detection alerts  
• Operating system log entries  
• Packets with unusual source addresses |
| DoS against an application on a particular host | • User reports of application unavailability  
• Network and host intrusion detection alerts  
• Application log entries  
• Packets with unusual source addresses |
**Template 14: Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP)**

**Disaster Recovery Plan (DRP)**
A Disaster Recovery Plan (DRP) specifies emergency response procedures, including specifying individual responsibility for responding to emergency situations and specifying procedures to enable team members to communicate with each other and with management during and after an emergency.

**RDP Classification**
Information system criticality and mission importance for the DRP is the same Mission Assurance Category (MAC) levels as defined in Annex 4: Baseline Security Categorization Guidelines.

**DRP Scoping Requirements**
The DRP requirements for critical assets are summarized below:

<table>
<thead>
<tr>
<th>Criticality</th>
<th>MAC I</th>
<th>MAC II</th>
<th>MAC III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted</td>
<td>High security required; must be in DRP</td>
<td>High security required; must be in DRP</td>
<td>High security required; must be in DRP</td>
</tr>
<tr>
<td>Confidential</td>
<td>Moderate security required; may be in DRP</td>
<td>Moderate security required; need not be in DRP</td>
<td></td>
</tr>
<tr>
<td>Internal Use</td>
<td>Minimal security required; may be in DRP</td>
<td>Minimal security required; need not be in DRP</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>Minimal security required; may be in DRP</td>
<td>Minimal security required; need not be in DRP</td>
<td></td>
</tr>
</tbody>
</table>

Backup copies of data and software that are sufficient for recovery from an emergency situation pertaining to critical assets must be stored at a secure, external site providing standard protection against hazards such as fire, flood, earthquake, theft, and decay. Requirements and procedures for such offsite backup shall be included in the DRP, including procedures and authorities for obtaining access to such sites in the event of an emergency.

Disaster recovery requirements should be specified when establishing maintenance agreements with vendors supplying components of critical resources. Ensure that vendors can provide replacement components within a reasonable period of time when planning system upgrades or deployments.

**Data Backup Availability**
Backup copies of data and software must be sufficient to satisfy DRP requirements, application or other critical information asset processing requirements, and any functional requirements of any critical information asset custodian dependent upon such data. Backup copies for disaster recovery purposes must be stored at a secure, off-site location that provides industry-standard protection. These backup requirements extend to all information systems and data necessary to be reconstituted in the event of a disaster.