Your Logo
Will Be
Placed Here

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

ACME Business Solutions, Inc.

NIST

WISP
Written Information Security Program
NIST 800-53 Rev 4

Table of Contents

WRITTEN INFORMATION SECURITY PROGRAM (WISP) OVERVIEW

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, Inc. (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective cybersecurity is a team effort involving the participation and support of every ACME user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

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

C-I-A
TRIAD
CONFIDENTIALITY
INTEGRITY
AVAILABILITY

- **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.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and information 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 Cybersecurity 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.

Appendix E: 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. Procedures for requesting an exception to policies, procedures or standards are available in Appendix F: Cybersecurity Exception Request Procedures.

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.

CYBERSECURITY PROGRAM STRUCTURE

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Cybersecurity documentation is comprised of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirement; procedures that must be followed; and guidelines that are recommended, but not mandatory.

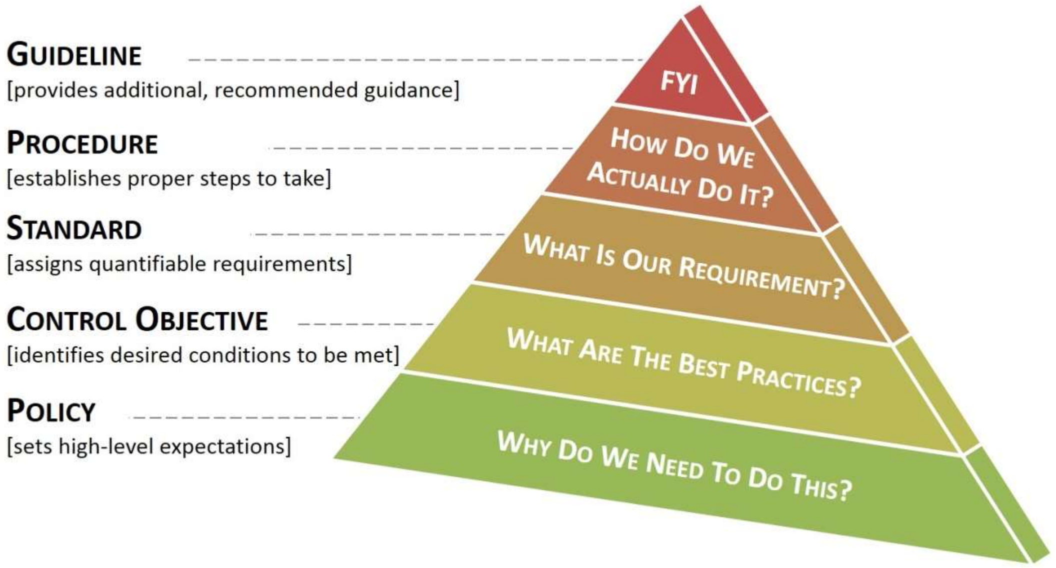

GUIDELINE
[provides additional, recommended guidance]
PROCEDURE
[establishes proper steps to take]
STANDARD
[assigns quantifiable requirements]
CONTROL OBJECTIVE
[identifies desired conditions to be met]
POLICY
[sets high-level expectations]
FYI
HOW DO WE ACTUALLY DO IT?
WHAT IS OUR REQUIREMENT?
WHAT ARE THE BEST PRACTICES?
WHY DO WE NEED TO DO THIS?

Figure 1: Cybersecurity Documentation Framework

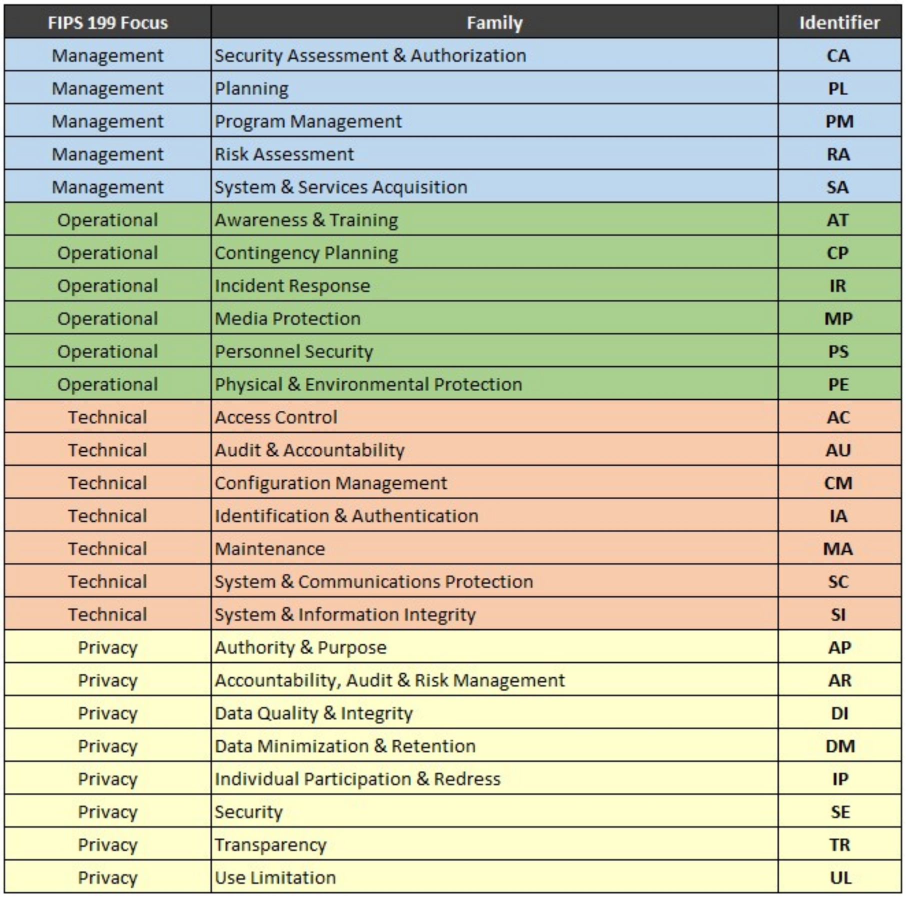
CYBERSECURITY CONTROL OBJECTIVES

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.[3] 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 Personally Identifiable Information (PII).
  - These dependent upon the proper functioning of the other classes of controls for their effectiveness and therefore require significant operational considerations.

[3] FIPS 199 - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

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.



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

Figure 2: NIST SP 800-53 Control Objectives Families & Identifiers

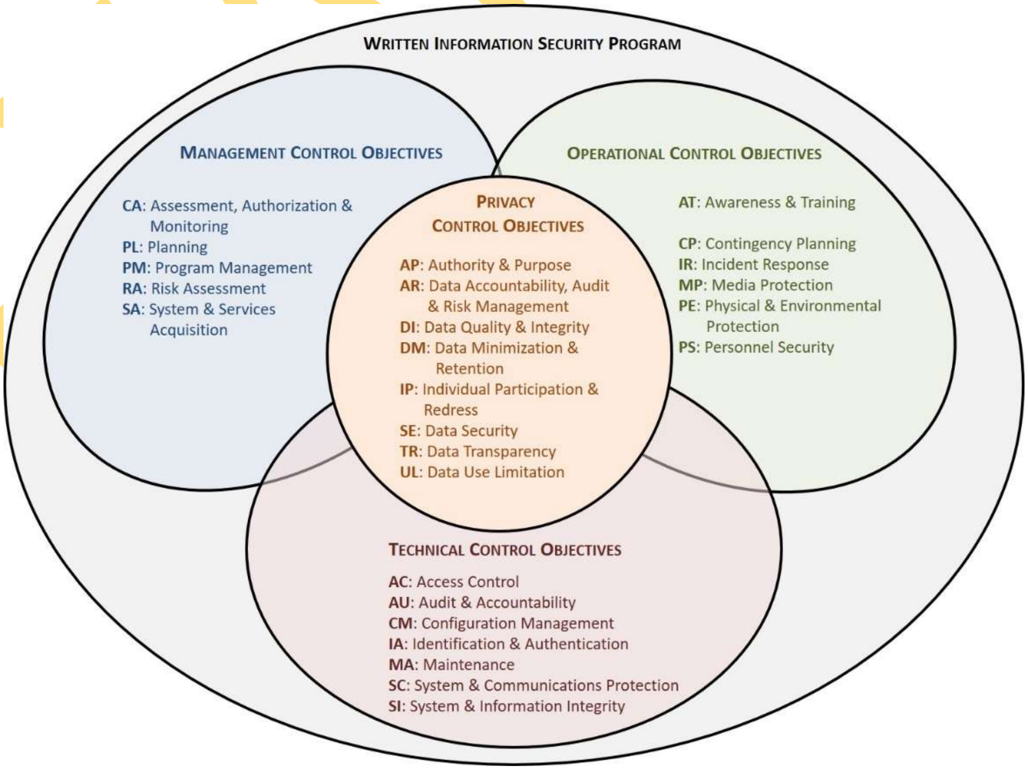

WRITTEN INFORMATION SECURITY PROGRAM
MANAGEMENT CONTROL OBJECTIVES
CA: Assessment, Authorization & Monitoring
PL: Planning
PM: Program Management
RA: Risk Assessment
SA: System & Services Acquisition
OPERATIONAL CONTROL OBJECTIVES
AT: Awareness & Training
CP: Contingency Planning
IR: Incident Response
MP: Media Protection
PE: Physical & Environmental Protection
PS: Personnel Security
PRIVACY CONTROL OBJECTIVES
AP: Authority & Purpose
AR: Data Accountability, Audit & Risk Management
DI: Data Quality & Integrity
DM: Data Minimization & Retention
IP: Individual Participation & Redress
SE: Data Security
TR: Data Transparency
UL: Data Use Limitation
TECHNICAL CONTROL OBJECTIVES
AC: Access Control
AU: Audit & Accountability
CM: Configuration Management
IA: Identification & Authentication
MA: Maintenance
SC: System & Communications Protection
SI: System & Information Integrity

Figure 3: NIST 800-53 Security Control Objective Relationships

CYBERSECURITY PROGRAM ACTIVITIES

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

Appendix G: Types of Security Controls provides a detailed description of cybersecurity considerations for protecting systems, based on the importance of the system and the sensitivity of the data processed or stored by the system.

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.

Security Assessments & Authorization (CA)

Security Assessment & Authorization Policy: ACME shall periodically assess systems to determine if Cybersecurity controls are effective and ensure Cybersecurity controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Management Intent: The purpose of the Security Assessment & Authorization (CA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to the ACME.

Supporting Documentation: Security Assessment & Authorization (CA)) control objectives & standards directly support this policy.

CA-01: Security Assessment & Authorization Policy & Procedures

Control Objective: The organization develops, disseminates, reviews, and updates:

- Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, and compliance; and
- Processes to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Standard: ACME is required to document cybersecurity assessment controls that, at a minimum, include:

(a) A formal, documented cybersecurity assessment procedure; and
(b) Processes to facilitate the implementation of cybersecurity assessments and authorizations.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA 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.

Enhancements: None

CA-02: Security Assessments

Control Objective: The organization:[4]

- Assesses the security controls in systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
- Produces a security assessment report that documents the results of the assessment; and
- Provides the results of the security control assessment, in writing, to the senior cybersecurity official or officially designated representative.

Standard: A formal cybersecurity risk analysis must be performed on all significant development and/or acquisitions, prior to systems being placed into production:

(a) New systems and applications must be appropriately tested for functionality prior to being placed in production; and
(b) Asset custodians and data/process owners are required to perform a gap analysis, at least once per year, to determine any deviations from their systems' current state of compliance and that which is required.

[4] MA201CMR17 17.03(2)(h) | OR646A.622(b)(B)(i)-(iv) | NIST CSF ID.RA-1, PR.IP-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5 & RS.CO-3

Supplemental Guidance: Security assessments should be performed on an ongoing basis since they are integral to identifying weaknesses, as well as validating that remediation actions were effective at eliminating or reducing vulnerabilities.

Control evaluators should have sufficient independence to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

Enhancements:

- CA-02(a) – Independent Assessors
- CA-02(b) – Specialized Assessments
- CA-02(c) – External Organizations

CA-02(a): Security Assessments | Independent Assessors

Control Objective: The organization employs assessors or assessment teams with independence to conduct security control assessments.

Standard: Whenever feasible, ACME shall utilize independent assessors for security assessment functions.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational systems under assessment or to the determination of security control effectiveness.

CA-02(b): Security Assessments | Specialized Assessments

Control Objective: The organization includes as part of security control assessments, specialized assessments that may include:

- In-depth monitoring;
- Vulnerability scanning;
- Malicious user testing;
- Insider threat assessment; and
- Performance/load testing.

Standard: Where technically feasible and justified by a valid business case, ACME shall utilize specialized assessments to address unique areas of risk.

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.

CA-02(c): Security Assessments | External Organizations

Control Objective: The organization accepts the results of external assessments by impartial, external organizations.

Standard: ACME shall accept the findings of assessments, when performed by impartial, external organizations with subject matter expertise in the area being assessed.

Supplemental Guidance: Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of supporting assessment documentation provided, or mandates imposed upon organizations by federal legislation, policies, or directives.

CA-03: Information System Connections

Control Objective: The organization allows connections only from authorized systems to connect to the Local Area Network (LAN).[5]

[5] NIST CSF ID.AM-3 & DE.AE-1

Risk Assessment (RA)

Risk Assessment Policy: ACME shall periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

Management Intent: The purpose of the Risk Assessment (RA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to ACME.

Supporting Documentation: Risk Assessment (RA) control objectives & standards directly support this policy.

RA-01: Risk Assessment Policy & Procedures

Control Objective: The organization develops, disseminates, reviews & updates: [33]

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

Standard: ACME is required to identify and document organization-wide security risk assessment controls that, at a minimum, include:

(a) A formal, documented security risk assessment policy; and
(b) Processes to facilitate the implementation of the security risk assessment policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA 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.

Enhancements: None

RA-02: Security Categorization

Control Objective: The organization:[34]

- Categorizes systems and data in accordance with applicable local, state, and Federal laws;
- Documents the security categorization results (including supporting rationale) in the security plan for systems; and
- Ensures the security categorization decision is reviewed and approved by the asset owner.

Standard: Based on the System Criticality and Data Sensitivity of a system (see Appendix D), asset custodians and data/process owners are required to:

(a) Categorize the system and data; and
(b) Where applicable, document the security categorization results (including supporting rationale) in a System Security Plan (SSP) for the system.

Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts on organizational operations, organizational assets, and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity, or availability. Security categorization processes carried out by business units, facilitates the development of inventories of information assets mappings to specific system components where information is processed, stored, or transmitted.

Enhancements: None

[33] MA201CMR17 17.03(2)(b) | NY DFS 500.09
[34] PCI DSS 9.6.1 | NIST CSF ID.AM-5, ID.RA-4 & ID.RA-5 | NY DFS 500.09

RA-03: Risk Assessment

Control Objective: The organization: [35]

- Conducts an annual assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system and the information it processes, stores, or transmits;
- Documents risk assessment results in an organization-approved format; and
- Reviews risk assessment results.

Standard: At least once per year or upon significant changes to the networks, ACME is required to conduct a formal cybersecurity risk assessment for the corporate network that, at the very least, covers the following:

(a) Identifies:
  i. Critical assets;
  ii. Potential natural and man-made threats;
  iii. Vulnerabilities;
(b) Documents known vulnerabilities in a formal risk assessment; and
(c) Assesses current cybersecurity controls affecting the confidentiality, integrity, and availability of critical data.

Supplemental Guidance: Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, and other organizations based on the operation and use of systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities).

Risk assessments (formal or informal) can be conducted at all three tiers in the risk management hierarchy (e.g., organization level, mission/business process level, or system level). RA-03 is noteworthy in that this control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework (RMF). Risk assessments can play an important role in security control selection processes particularly during the application of tailoring guidance, which includes security control supplementation.

Enhancements:

- RA-03(a) – Risk Ranking

RA-03(a): Risk Assessment | Risk Ranking

Control Objective: The organization will establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry-recognized leading practices. [36]

Standard: Asset custodians and data/process owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system.

Supplemental Guidance: The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

RA-04: Risk Assessment Update

Control Objective: The organization routinely updates its risk assessment and reacts accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.[37]

Standard: ACME is required to update risk assessments whenever there are significant changes to systems, the environment of operation, or other conditions that may impact the security state of the system.

Supplemental Guidance: None

Enhancements: None

[35] HIPAA 164.308(a)(1)(ii)(A) & (B) | GLBA Safeguards Rule | PCI DSS 12.2 | MA201CMR17 17.03(2)(b) | OR646A.622(b)(A)(ii) | NIST CSF ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, PR.IP-12, DE.AE-4 & RS.MI-3

[36] National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm

[37] GLBA Safeguards Rule | PCI DSS 6.1 | MA201CMR17 17.03(2)(i) & 17.03(2)(b)(c) | OR646A.622(b)(A)(iv)

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 directly support this policy.

AT-01: Security Awareness & Training Policy & Procedures

Control Objective: The organization develops, disseminates, reviews & updates: [63]

- 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, procedures and associated controls.

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

Enhancements: None

AT-02: Security Awareness

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. [64]

[63] NY DFS 500.14

[64] 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

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.

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.

Enhancements:

- AT-02(a) – Practical Exercises
- AT-02(b) – Insider Threat

AT-02(a): Security Awareness | Practical Exercises

Control Objective: The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.

Standard: ACME's Cybersecurity personnel are responsible for developing and implementing practical exercises in security awareness training that simulate actual cyber-attacks.

Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.

AT-02(b): Security Awareness | 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-03: Security Training

Control Objective: The organization provides role-based security-related training:[65]

- 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; and
(b) ACME's Cybersecurity personnel are required to provide training, at least annually, thereafter.

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

[65] PCI DSS 12.6.1 | 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

Technical Controls

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.

Access Control (AC)

Access Control Policy: ACME shall implement logical access controls to limit access to systems and processes to authorized users.

Management Intent: The purpose of the Access Control (AC) policy is to ensure that ACME limits access to its systems and data to authorized users.

Supporting Documentation: Access Control (AC) control objectives & standards directly support this policy.

AC-01: Access Control Policy & Procedures

Control Objective: The organization develops, disseminates, reviews & updates:[133]

- A formal, documented access control 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 access control policy and associated access controls.

Standard: ACME is required to document organization-wide access control controls that, at a minimum, include:

(a) A formal, documented access control policy; and
(b) Processes to facilitate the implementation of the access control policy, procedures and associated controls.

Supplemental Guidance: None

Enhancements: None

AC-02: Account Management

Control Objective: The organization manages system accounts, including: [134]

- Identifying account types (e.g., individual, group, system, application, guest/anonymous, and temporary);
- Establishing conditions for group membership;
- Identifying authorized users of the system and specifying access privileges;
- Requiring appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes;
- Deactivating accounts that are no longer required;
- Granting access to the system based on a valid access authorization; and
- Reviewing accounts on a regular basis.

Standard: ACME's IT department is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion, and modification of user IDs, credentials, and other identifier objects to ensure authorized use is maintained;
(b) Verify user identity before issuing initial passwords or performing password resets;
(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;
(d) Immediately revoke access for any terminated users;
(e) Remove/disable inactive user accounts within ninety (90) days;
(f) Limit repeated access attempts by locking out the user ID after not more than six (6) attempts;

[133] HIPAA 164.312(a)(a) | PCI DSS 8.1 & 8.4

[134] HIPAA 164.312(d) | PCI DSS 8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 & 8.7 | MA201CMR17 17.04(1(a) | NIST CSF PR.AC-1, PR.AC-4, DE.CM-1 & DE.CM-3

(g) Set the lockout duration to a minimum of thirty (30) minutes or until administrator enables the user ID;

(h) Establish and administer accounts in accordance with a role-based access scheme that organizes system and network privileges into roles;

(i) Track and monitors role assignments for privileged user accounts;

(j) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;

(k) Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;

(l) Minimize the use of group, shared, or generic accounts and passwords;

(m) Default user IDs and accounts are disabled or removed;

(n) Service providers with remote access to ACME's premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer; and

(o) Restrict user direct access or queries to databases to database administrators, including:

  i. Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);

  ii. Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators; and

  iii. Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

Supplemental Guidance:

- Access privileges granted to general users should be reviewed by information owners every six (6) months to determine if access rights are commensurate with the user's job duties.
- Evidence of account and privilege reviews that documents the review occurred, who conducted the review, and what action (if any) was taken should be maintained for a period of twelve (12) months.
- Asset custodians and data/process owners are required to promptly report all changes in user duties or employment status for the User IDs associated with the involved personnel and administrators should promptly revoke all unnecessary access privileges

Enhancements:

- AC-02(a) – Automated System Account Management
- AC-02(b) – Removal of Temporary / Emergency Accounts
- AC-02(c) – Disable Inactive Accounts
- AC-02(d) – Automated Audit Actions
- AC-02(e) – Inactivity Logout
- AC-02(f) – Roles Based Schemes (Role-Based Access Control (RBAC))
- AC-02(g) – Restrictions on Shared Groups / Accounts
- AC-02(h) – Shared / Group Account Credential Termination

AC-02(a): Account Management | Automated System Account Management

Control Objective: The organization employs automated mechanisms to support the management of information system accounts.

Standard: Where technically feasible, automated mechanisms are required to be configured to automatically alert appropriate personnel for security-related changes in account status.

Supplemental Guidance: The use of automated mechanisms can include, for example:

- Using email or text messaging to automatically notify account managers when users are terminated or transferred;
- Using the information system to monitor account usage; and
- Using telephonic notification to report atypical system account usage.

AC-02(b): Account Management | Removal of Temporary / Emergency Accounts

Control Objective: The information system automatically disables or removes temporary and emergency accounts after an organization-defined time period for each type of account.

Standard: Where technically feasible, automated mechanisms are required to disable temporary / emergency accounts after twenty-four (24) hours.

Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.

AC-02(c): Account Management | Disable Inactive Accounts

Control Objective: The information system automatically disables inactive accounts after an organization-defined time period.

Standard: Where technically feasible, automated mechanisms are required to disable inactive accounts after ninety (90) days.

Supplemental Guidance: None

AC-02(d): Account Management | Automated Audit Actions

Control Objective: The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies organization-defined personnel or roles.

Standard: Where technically feasible, automated mechanisms are required to alert asset custodians when accounts are created, modified, enabled, disabled, and/or removed.

Supplemental Guidance: None

AC-02(e): Account Management | Inactivity Logout

Control Objective: The organization requires that users log out after an organization-defined time period of expected inactivity.

Standard: If a session has been idle for more than fifteen (15) minutes, the user must be logged out and required to re-authenticate to re-activate the session.

Supplemental Guidance: None

AC-02(f): Account Management | Role Based Schemes (Role-Based Access Control (RBAC))

Control Objective: The organization: [135]

- Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
- Monitors privileged role assignments; and
- Takes actions when privileged role assignments are no longer appropriate.

Standard: ACME is required to establish Role-Based Access Control (RBAC) access enforcement via Active Directory (AD) that:

(a) Covers all system components;
(b) Assigns privileges to individuals based on job classification and function; and
(c) Restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Supplemental Guidance: RBAC is a type of Discretionary Access Control (DAC).

AC-02(g): Account Management | Restrictions on Shared Groups / Accounts

Control Objective: The organization only permits the use of shared/group accounts that meet conditions for establishing shared/group accounts.

Standard: Only when justified by a valid business case, ACME permits the use of shared/group accounts.

Supplemental Guidance: None

AC-02(h): Account Management | Shared / Group Account Credential Termination

Control Objective: The information system terminates shared/group account credentials when members leave the group.

Standard: When members no longer need access to a shared/group account, permissions are changed on all affected information systems in a timely manner.

Supplemental Guidance: None

[135] HIPAA 164.308(a)(4(ii)(A) & (B) & (C) | PCI DSS 7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3

AC-03: Access Enforcement

Control Objective: Systems enforce approved authorizations for logical access to the system in accordance with applicable policy.[136]

Standard: ACME is required to limit access to systems and sensitive data to only those individuals whose job requires such access.

Enhancements: Access limitations should include the following:

- Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities;
- Assignment of privileges is based on individual personnel's job classification and function;
- Requirement for a documented approval by authorized parties specifying required privileges; and
- Implementation of an automated access control system.

AC-04: Information Flow Enforcement – Access Control Lists (ACLs)

Control Objective: Systems enforce approved authorizations for controlling the flow of information within a system and between interconnected systems in accordance with applicable policy.[137]

Standard: Network administrators are required to enforce information flow control using:

(a) Access Control Lists (ACL) as a basis for flow control decisions;
(b) Documented business justification for the use if all services, protocols, and ports allowed;
(c) Explicit security attributes on information, source, and destination objects as a basis for flow control decisions;
(d) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [138]
(e) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [139]
(f) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [140]
(g) Unauthorized outbound traffic to the Internet is prohibited; [141]
(h) Stateful inspection (dynamic packet filtering) must be implemented; [142]
(i) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [143] and
(j) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [144]

Supplemental Guidance: None

Enhancements:

- AC-04(a) – Object Security Attributes
- AC-04(b) – Content Check for Encrypted Data
- AC-04(c) – Embedded Data Types
- AC-04(d) – Metadata
- AC-04(e) – Human Reviews
- AC-04(f) – Physical / Logical Separation for Information Flows

AC-04(a): Information Flow Enforcement | Object Security Attributes

Control Objective: The information system uses security attributes associated with information, source, and destination objects to enforce defined information flow control policies as a basis for flow control decisions.

Standard: Data/process owners and asset custodians are required to use security attributes associated with information, source, and destination objects to enforce defined information flow control policies as a basis for flow control decisions.

[136] HIPAA 164.308(a)(4(i) & (ii) | PCI DSS 7.1, 7.1.1-7.1.4, 7.2, 7.2.1 & 7.2.3 | MA201CMR17 17.04(1)(b) & 17.04(b)(a) | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.AM-3, PR.AC-4 & PR.PT-3
[137] PCI DSS 1.1.6, 1.3.3 & 1.3.5 | OR646A.622(2)(d)(C)(iii) | NIST CSF PR.AC-5, PR.DS-5, PR.PT-4 & DE.AE-1
[138] PCI DSS 1.3.1
[139] PCI DSS 1.3.2
[140] PCI DSS 1.3.3
[141] PCI DSS 1.3.4
[142] PCI DSS 1.3.5
[143] PCI DSS 1.3.6
[144] PCI DSS 1.3.7

System & Communication Protection (SC)

System & Communication Protection Policy: ACME shall employ industry-recognized leading practice principles that promote effective Cybersecurity within systems and the network.

Management Intent: The purpose of the System & Communication Protection (SC) policy is to ensure sufficient protections are in place to protect the confidentiality and integrity of ACME’s communications.

Supporting Documentation: System & Communication Protection (SC) control objectives & standards directly support this policy.

SC-01: System & Communication Policy & Procedures

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

- A formal, documented system and communications protection 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 system and communications protection policy and associated system and communications protection controls.

Standard: ACME is required to document organization-wide system and communication controls that, at a minimum, include:

(a) A formal, documented system and communication policy; and
(b) Processes to facilitate the implementation of the system and communication policy, procedures, and associated controls.

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC 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.

Enhancements: None

SC-02: Application Partitioning

Control Objective: System configurations separate user functionality (including user interface services) from system management functionality.[218]

Standard: Where technically feasible, physically or logically separate user interfaces (e.g., public Web pages) are required to be implemented from storage and management services (e.g., administrative or database management). Separation may be accomplished through the use of one or more of the following:

(a) Network segmentation;
(b) Different computers;
(c) Different central processing units;
(d) Different instances of the operating system;
(e) Different network addresses; or
(f) Other methods as appropriate.

Supplemental Guidance: System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

Enhancements: None

[218] PCI DSS 11.3.4

SC-03: Security Function Isolation

Control Objective: System configurations isolate security functions from non-security functions.[219]

Standard: Asset custodians and data/process owners are required to implement isolation techniques to prevent functions that require different security levels from co-existing on the same server. Isolation techniques include, but are not limited to:

(a) Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server;
(b) Firewall and router configurations need be configured to restrict connections between untrusted networks and any system components in ACME's trusted, internal network;
(c) Firewall need be installed at all connections from an internal to any other internal or external network;
(d) Demilitarized Zones (DMZs) need to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;
(e) Servers which access external networks or are accessed from external networks need to be logically isolated from the private Intranet;
(f) Networks need to be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices;
(g) Switched network technology need to be utilized, when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic;
(h) Trust relationships should be strictly avoided between information resources with different risk profiles; and
(i) Information resources with higher protection requirements for confidentiality should not have a trusted relationship with a system that has lower protection requirements.
(j) If segmentation is used to isolate the sensitive networks from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.[220]

Supplemental Guidance: The system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities.

Enhancements:

- SC-03(a) – Layered Defenses

SC-03(a): Security Function Isolation | Layered Defenses

Control Objective: The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.[221]

Standard: ACME is required to use a Defense-in-Depth (DiD) architecture to protect the Confidentiality, Integrity, and Availability of systems and data, placing systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.

Supplemental Guidance: The implementation of layered structures with minimized interactions among security functions and non-looping layers (e.g., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.

SC-04: Information In Shared Resources

Control Objective: Systems prevent unauthorized and unintended information transfer via shared system resources.

Standard: Asset custodians and data/process owners are required to ensure that systems are configured to require privilege levels for access. The levels must ensure data is not exposed to individuals or processes with a lower privilege level.

[219] PCI DSS 1.2, 1.3.1, 2.2.1 & 11.3.4
[220] PCI DSS 11.3.4 & 11.3.4.1
[221] PCI DSS 1.3.7

Supplemental Guidance: This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resource have been released back to systems. The control of information in shared system resources is also referred to as object reuse.

Enhancements: None

SC-05: Denial of Service (DoS) Protection

Control Objective: Systems protect against or limit the effects of denial of service attacks.[222]

Standard: Technology architects, asset custodians, and data/process owners are required to configure the architecture of the network and systems to ensure the capability exists to limit the effects of denial of service attacks.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

Enhancements: None

SC-06: Resource Priority

Control Objective: Systems limit the use of resources by priority.

Standard: Asset custodians and data/process owners are required to prioritize resources to prevent or limit Denial of Service (DoS) attack effectiveness.

Supplemental Guidance: Priority protection helps prevent lower-priority processes from delaying or interfering with the system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to system components for which there are only single users/roles.

Enhancements: None

SC-07: Boundary Protection

Control Objective: The organization employs boundary protection mechanisms to separate system components directly supporting organization-defined missions and/or business functions. [223]

Standard: Network administrators are required to:

(a) Implement a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the internal network zone;
(b) Verify that the current network diagrams are consistent with the firewall configuration standards;
(c) Prohibit direct public access between the Internet and any sensitive system in the internal network zone;
(d) Restrict inbound and outbound traffic to that which is necessary for authorized business purposes;
(e) Limit the number of access points to the system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic;
(f) Ensure traffic flow policies are established and reviewed for each managed interface;
(g) Ensure the exceptions to Access Control Lists (ACLs) are documented and reviewed;
(h) Ensure systems prevent remote devices that have established a non-remote connection (e.g., VPN) with the system from communicating outside that path and with resources external to the network;
(i) Ensure systems prevent the unauthorized release of information outside the system boundary or any unauthorized communication through the system boundary when there is an operational failure of the boundary protection mechanisms;
(j) Ensure private IP addresses and routing information are not disclosed to unauthorized parties; and

[222] NIST CSF PR.DS-4 & DE.CM-1

[223] PCI DSS 1.1.3, 1.1.4, 1.2.1, 1.2.3 & 1.3 | MA201CMR17 17.04(6) | NIST CSF PR.AC-5, PR.DS-5, PR.PT-4 & DE.CM-1

Standard: Where technically feasible, ACME shall incorporate the detection of unauthorized security-relevant changes to the information system into ACME's incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.

SI-08: Spam Protection

Control Objective: The organization:

- Employs spam protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
- Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

Standard: ACME is required to centrally manage spam protection mechanisms, including signature definitions, in an effort to reduce the introduction of malicious software to client systems.

Supplemental Guidance: System entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

Enhancements:

- SI-08(a) – Central Management
- SI-08(b) – Automatic Updates

SI-08(a): Spam Protection | Central Management

Control Objective: The organization centrally manages spam protection mechanisms.

Standard: Where technically feasible, ACME shall centrally manage the spam protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.

SI-08(b): Spam Protection | Automatic Updates

Control Objective: The information system automatically updates spam protection mechanisms.

Standard: Where technically feasible, information systems must automatically update spam protection mechanisms.

Supplemental Guidance: None

SI-09: Information Input Restrictions

Control Objective: The organization restricts the capability to input information to systems to authorized personnel.

Standard: On custom-developed applications and web pages, asset custodians and data/process owners are required to enforce rules to require inputs to be prescreened to prevent the content from being unintentionally interpreted as commands.

Supplemental Guidance: Input restrictions are important to prevent against common hacking techniques that take advantage of poor software development principles (e.g., SQL injection and buffer overflow attacks).

Enhancements: None

SI-10: Input Data Validation

Control Objective: Systems check the validity of information inputs.

DM-02(b): Data Retention & Disposal | Sensitive Data Storage

Control Objective: The organization limits storing sensitive data to explicit business requirements.[260]

Standard: Personally Identifiable Information (PII) is prohibited from being stored for any longer than the legitimate business need exists to retain the data.

Supplemental Guidance: For credit or debit cardholder data, ACME is required to not store:

- Sensitive authentication data after authorization, even if it is encrypted;
- The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data;
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions; or
- The personal identification number (PIN) or the encrypted PIN block.

In the normal course of business, the following data elements from the magnetic stripe may need to be retained (To minimize risk, store only these data elements as needed for business):

- The cardholder's name;
- Primary account number (PAN);
- Expiration date; or
- Service code

DM-02(c): Data Retention & Disposal | Data Masking

Control Objective: The organization applies data masking to sensitive information that is displayed or printed.[261]

Standard: Sensitive information that is displayed or printed is required to be masked. This includes, but is not limited to:

(a) Financial account numbers;
(b) Social Security Numbers (SSN); and
(c) Credit or debit Primary Account Numbers (PANs) (no more than the first six and last four digits allowed).

Supplemental Guidance: Only personnel with a legitimate business need should be able to see more than the first six/last four of the PAN.

DM-03: Minimization Of PII Used In Testing, Training & Research

Control Objective: The organization:

- Develops policies and procedures for the use of PII for testing, training, and research; and
- Implements controls to protect PII used for testing, training, and research.

Standard: The use of PII is prohibited for research, testing or training.

Supplemental Guidance: Organizations often use PII for testing new applications or systems prior to deployment. Organizations also use PII for research purposes, such as statistical analysis, and for training.

Enhancements: None

[260] PCI DSS 3.2 & 3.2.1-3.2.3

[261] PCI DSS 3.3

Individual Participation & Redress (IP)

Individual Participation & Redress Policy: ACME shall enable individuals to be active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Management Intent: The purpose of the Individual Participation & Redress (IP) policy is to addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their Personally Identifiable Information (PII).

Supporting Documentation: Individual Participation & Redress (IP) control objectives & standards directly support this policy.

IP-01: Consent

Control Objective: The organization:

- Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
- Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
- Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
- Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to support itemized or tiered consent for specific uses of data.

Supplemental Guidance: Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase the risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices.

Enhancements: None

IP-02: Individual Access

Control Objective: The organization provides individuals the ability to have access to their Personally Identifiable Information (PII).[262]

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to support access requests to users' PII.

Supplemental Guidance: Access includes timely, simplified, and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. Legal counsel should be consulted for record request processing.

Enhancements: None

IP-03: Redress

Control Objective: The organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate.

Standard: Where technically feasible and a business reason exists, data/process owners are required to implement mechanisms to address end user redress issues.

[262] Argentina Personal Data Protection Law #25.326 & Regulatory Decree # 1558/2001 (PDPL)

Appendices

Appendix A: Data Classification & Handling Guidelines

A-1: 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:

Classification	Data Classification Description	
Restricted	Definition	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.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME. · 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.
Confidential	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by ACME
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
Internal Use	Definition	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.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME. · Impact could include damaging the company's reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to ACME. · Impact would not be damaging or a risk to business operations.

A-2: 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.

PUBLIC
Public Release Authorized

INTERNAL USE
Access Limited to Internal Use Only

CONFIDENTIAL
Access Limited to Authorized Personnel

RESTRICTED
Access Limited to Authorized Personnel

A-3: 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.

A-4: Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
  - Passport number
  - Permanent resident card
- Driver License (DL)
- Financial account number
  - Payment card number (credit or debit)
  - Bank account number
- Electronic Protected Health Information (ePHI)

A-5: Personal Information (PI)

PI 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.

PII is always PI, but PI is not always PII. Examples of PI 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;

A-6: Data Handling Guidelines

Handling Controls	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-ACME employees.	▪ NDA is recommended prior to access by non-ACME employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ 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	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ 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	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*

Appendix B: 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.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	

E-3: Cybersecurity Work Roles & Responsibilities

Work roles are the most detailed groupings of cybersecurity and related work which include a list of attributes required to perform that role in the form of Knowledge, Skills, and Abilities (KSAs) and tasks performed in that role.

Work being performed in a job or position is described by selecting one or more work roles from the NICE Framework relevant to that job or position, in support of mission or business processes. To aid in the organization and communication about cybersecurity responsibilities, work roles are grouped into specific classes of categories and specialty areas.

Category	Specialty Area	Work Role	Work Role ID	Work Role Description
Securely Provision (SP)	Risk Management (RSK)	Authorizing Official/Designating Representative	SP-RSK-001	Senior official or executive with the authority to formally assume responsibility for operating a system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations.
		Security Control Assessor	SP-RSK-002	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).
	Software Development (DEV)	Software Developer	SP-DEV-001	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
		Secure Software Assessor	SP-DEV-002	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.
		Security Architect	SP-ARC-002	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
	Technology R&D (TRD)	Research & Development Specialist	SP-TRD-001	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
	Systems Requirements Planning (SRP)	Systems Requirements Planner	SP-SRP-001	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.
	Test and Evaluation (TST)	System Testing and Evaluation Specialist	SP-TST-001	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.
		Systems Security Developer	SP-SYS-001	Designs, develops, tests, and evaluates system security throughout the systems development life cycle.

Appendix H: Rules of Behavior / User Acceptable Use

These Rules of Behavior apply to the use of ACME-provided IT resources, regardless of the geographic location:

- Data and system use must comply with ACME policies and standards.
- Unauthorized access to data and/or systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information, including Personally Identifiable Information (PII).

H-1: Acceptable Use

Users shall:

- In accordance with organizational procedures, immediately report all lost or stolen equipment, known or suspected security incidents, known or suspected security policy violations or compromises, or suspicious activity. Known or suspected security incidents are inclusive of an actual or potential loss of control or compromise, whether intentional or unintentional, of authenticator, password, or sensitive information, including PII, maintained or in possession of the user.
- Ensure that software, including downloaded software, is properly licensed, free of malicious code, and authorized before installing and using it on organization-owned systems.
- Log off or lock systems when leaving them unattended.
- Complete security awareness training before accessing any system and on an annual basis thereafter. Permit only authorized users to use organization-provided systems.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Sanitize or destroy electronic media and papers that contain sensitive data when no longer needed, in accordance with organization records management and sanitization policies, or as otherwise directed by management.
- Only access sensitive information necessary to perform job functions (e.g., need to know).
- Use PII only for the purposes for which it was collected, to include conditions set forth by stated privacy notices and published notices.
- Ensure the accuracy, relevance, timeliness, and completeness of PII, as is reasonably necessary.
- Wear organization-issued identification badges at all times in organization-operated facilities.

H-2: Prohibited Use

Users shall not:

- Direct or encourage others to violate organizational policies, procedures, standards or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user’s account, identity, or password.
- Exceed authorized access to sensitive information.
- Cause congestion, delay, or disruption of service to any organization-owned IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, as does some uses of “push” technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.
- Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Use organization-provided IT resources for commercial purposes or in support of “for-profit” activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- Establish unauthorized personal, commercial or non-profit organizational web pages on organization-provided systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.

ANNEX 1 - CYBERSECURITY POLICIES SUMMARY

Policy #	FIPS 199 Focus	Family	Identifier
1	Management	Security Assessment & Authorization	**CA**
2	Management	Planning	**PL**
3	Management	Program Management	**PM**
4	Management	Risk Assessment	**RA**
5	Management	System & Services Acquisition	**SA**
6	Operational	Contingency Planning	**CP**
7	Operational	Incident Response	**IR**
8	Operational	Media Protection	**MP**
9	Operational	Awareness & Training	**AT**
10	Operational	Personnel Security	**PS**
11	Operational	Physical & Environmental Protection	**PE**
12	Technical	Access Control	**AC**
13	Technical	Audit & Accountability	**AU**
14	Technical	Configuration Management	**CM**
15	Technical	Identification & Authentication	**IA**
16	Technical	Maintenance	**MA**
17	Technical	System & Communications Protection	**SC**
18	Technical	System & Information Integrity	**SI**
19	Privacy	Authority & Purpose	**AP**
20	Privacy	Accountability, Audit & Risk Management	**AR**
21	Privacy	Data Quality & Integrity	**DI**
22	Privacy	Data Minimization & Retention	**DM**
23	Privacy	Individual Participation & Redress	**IP**
24	Privacy	Security	**SE**
25	Privacy	Transparency	**TR**
26	Privacy	Use Limitation	**UL**

POLICY STATEMENT 1: SECURITY ASSESSMENT & AUTHORIZATION (CA)

Management Intent: The purpose of the Security Assessment & Authorization (CA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to the ACME.

Security Assessment & Authorization Policy: ACME shall periodically assess systems to determine if Cybersecurity controls are effective and ensure Cybersecurity controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Supporting Documentation: Security Assessment & Authorization (CA) control objectives & standards directly support this policy.

POLICY STATEMENT 2: PLANNING (PL)

Management Intent: The purpose of the Planning (PL) policy is to ensure due care planning considerations are addressed to minimize risks to ACME.

Planning Policy: ACME shall develop, document, implement, and periodically update measures to protect its critical systems.

Supporting Documentation: Planning (PL) control objectives & standards directly support this policy.

Policy Statement 3: Program Management (PM)

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.

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

Supporting Documentation: Program Management (PM) control objectives & standards directly support this policy.

Policy Statement 4: Risk Assessment (RA)

Management Intent: The purpose of the Risk Assessment (RA) policy is to ensure that risk determinations made during the initial risk assessment for a project or system are accurate and provide a thorough portrayal of the risks to ACME.

Risk Assessment Policy: ACME shall periodically assess the risk to operations, assets, and data, resulting from the operation of systems and the associated processing, storage, or transmission of data.

Supporting Documentation: Risk Assessment (RA) control objectives & standards directly support this policy.

Policy Statement 5: System & Services Acquisition (SA)

Management Intent: The purpose of the System & Services Acquisition (SA) policy is to ensure that systems employ a System Development Life Cycle (SDLC), where the security of systems and services are assessed throughout the operational life of the systems to reduce risks to ACME.

System & Services Acquisition Policy: ACME shall allocate sufficient resources to adequately protect organizational systems by employing a System Development Life Cycle (SDLC) process that incorporate Cybersecurity considerations.

Supporting Documentation: System & Service Acquisition (SA) control objectives & standards directly support this policy.

Policy Statement 6: Awareness & Training (AT)

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

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.

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

Policy Statement 7: Contingency Planning (CP)

Management Intent: The purpose of Contingency Planning (CP) policy is to establish procedures that will help ACME management to quickly determine the appropriate actions to be taken due to an interruption of service or disaster.

Contingency Planning Policy: ACME shall establish, implement and maintain plans for the continuity of operations (COOP) in emergency situations to ensure the availability of critical information resources.

Supporting Documentation: Contingency Planning (CP) control objectives & standards directly support this policy.

Written Information Security Program (WISP)

FORMS, TEMPLATES & REFERENCES

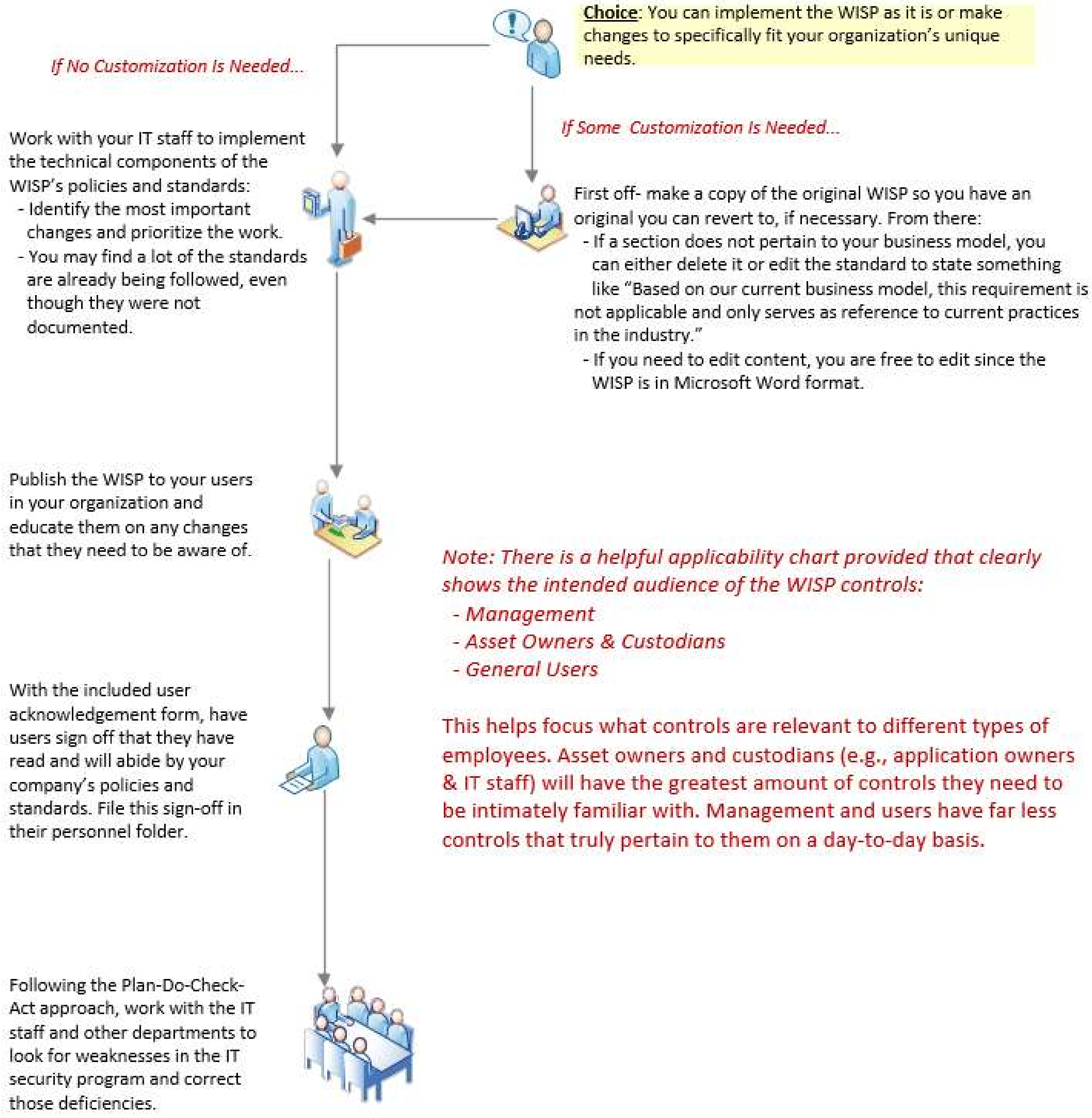
WISP

Written Information Security Program

Table of Contents

WISP IMPLEMENTATION OVERVIEW

The diagram depicted below is an illustration of the process flow that generally takes place to implement a Written Information Security Program (WISP) within an organization. There will most likely be some level of customization of the WISP that is necessary to meet [Company Name]'s unique requirements and staffing levels.



Choice: You can implement the WISP as it is or make changes to specifically fit your organization's unique needs.

If No Customization Is Needed...

Work with your IT staff to implement the technical components of the WISP's policies and standards:
- Identify the most important changes and prioritize the work.
- You may find a lot of the standards are already being followed, even though they were not documented.

If Some Customization Is Needed...

First off- make a copy of the original WISP so you have an original you can revert to, if necessary. From there:
- If a section does not pertain to your business model, you can either delete it or edit the standard to state something like "Based on our current business model, this requirement is not applicable and only serves as reference to current practices in the industry."
- If you need to edit content, you are free to edit since the WISP is in Microsoft Word format.

Publish the WISP to your users in your organization and educate them on any changes that they need to be aware of.

Note: There is a helpful applicability chart provided that clearly shows the intended audience of the WISP controls:
- *Management*
- *Asset Owners & Custodians*
- *General Users*

This helps focus what controls are relevant to different types of employees. Asset owners and custodians (e.g., application owners & IT staff) will have the greatest amount of controls they need to be intimately familiar with. Management and users have far less controls that truly pertain to them on a day-to-day basis.

With the included user acknowledgement form, have users sign off that they have read and will abide by your company's policies and standards. File this sign-off in their personnel folder.

Following the Plan-Do-Check-Act approach, work with the IT staff and other departments to look for weaknesses in the IT security program and correct those deficiencies.

Written Information Security Program (WISP) Implementation

[Official Company Name] ([Company Name]) is committed to protecting its employees, partners, clients and [Company Name] from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every [Company Name] user who interacts with data and information systems. The reason for implementing [Company Name]'s Written Information Security Program (WISP) is not to impose restrictions that are contrary to [Company Name]'s established culture of openness, trust, and integrity, but to strengthen [Company Name]'s ability to guard against unauthorized access to, alteration, disclosure or destruction of data and information systems. This also includes against accidental loss or destruction.

The purpose of the Written Information Security Program is to ensure that security controls are properly implemented and that clients and business partners are confident their information is adequately protected. Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Therefore, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – This security component addresses preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – This security component addresses the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – This security component addresses ensuring timely and reliable access to and use of information.

The WISP establishes the foundation for the Information Security Program at [Company Name] . The formation of the policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which [Company Name] shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related procedures, standards, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure [Company Name] 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 [Company Name] comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of [Company Name] data.

It is the responsibility of every user to know these policies and to conduct their activities accordingly. The WISP is effective as of [enter date policy is effective].

Respectfully,

[owner/manager's signature]
[insert owner/manager's printed name]
[insert owner/manager's title]

[Official Company Name]
([Company Name])

Written Information Security Program Acknowledgement

I, ____, acknowledge I have read [Company Name]'s Written Information Security Program (WISP). I agree to abide by [Company Name]'s policies, standards, and procedures.

I acknowledge that if I do have any questions regarding any information within [Company Name]'s WISP, it is my responsibility to address those issues with my manager for further clarification. I acknowledge that ignorance on my part is not an excuse and I take full responsibility for my actions and the actions I fail to do. I acknowledge and understand that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I agree to indemnify, defend and hold harmless [Company Name] , its subsidiaries and affiliated companies, and each of its respective owners, officers, directors, managers, employees, shareholders and agents (each an "indemnified party" and, collectively, "indemnified parties") from and against any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), and expenses (including, but not limited to, reasonable attorney's fees) threatened, asserted or filed by a third-party against any of the indemnified parties arising out of or relating to any and all gross negligence and/or misconduct on my part.

The terms of this acknowledgment shall survive any termination of employment.

_______________________________	_______________________________
User Name / Title	**Signature & Date**
_______________________________	_______________________________
User's Supervisor / Manager	**Signature & Date**

WISP TEMPLATE 5: INCIDENT RESPONSE FORM

[Official Company Name]
([Company Name])

Incident Response Form

Incident Report					
System:		**Date:**		**Time:**	
Submitted By:		**Location:**			
Submitted To (supervisor's name):					
Description of Problem (Who, What, Where, When, Why, and How)					
Damage Assessment					
Steps Taken to Restore Service / Remedy Problem					
Time Required to Restore Service / Remedy Problem					
Resources Used					
Changes Requested / Needed to Update Information Security Procedures					

WISP TEMPLATE 7: ADMINISTRATOR ACCOUNT REQUEST FORM

[Official Company Name]
([Company Name])

Administrator Account Request Form

INSTRUCTIONS
Completed forms should be submitted to your primary supervisor. Your supervisor will forward this to the IT department.

End User Name: ____________________ Phone: ____________________

Department: ____________________ Email Address: ____________________

Type of Rights: □ Domain Administrator □ Local Administrator □ Power User □ Other

Request Reason(s):

Requestor Signoff

As the end user specified on this form, I certify that the information provided in this document is both true and accurate.

The end user also recognizes the increased responsibilities inherent to having an account with elevated privileges and will follow all policies, procedures, standards, and guidelines required by [Company Name] users with administrative rights. Failure to follow these standards will result in immediate revocation of elevated privileges.

End User Signature **X** Date: / /

Requestor's Supervisor

Completed By: (print name) Signature: **X** Date Received: / /

Information Security Officer (ISO)

Received Bv: (print name) Signature: **X** Date Received: / /

The expiration date of elevated privileges (if applicable): ____________________

WISP TEMPLATE 13: INCIDENT RESPONSE PLAN (IRP) TEMPLATE

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

Malicious Actions	Possible Indications of an Incident
Denial of Service (DoS) Examples	**You might be experiencing a DoS if you see…**
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

ESCALATION LEVEL CONSIDERATIONS

Incident Response management must consider several characteristics of the incident before escalating the response to a higher level. These considerations include:

- Legal requirements for breach notification?
- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact of [Company Name] ?
- Will this negatively affect [Company Name]'s image?

INCIDENT RESPONSE PROCESS

The Incident Response Process is an escalation process whereas the impact of the incident becomes more significant or widespread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.

Step		Responsible Entity	Incident Response Plan (IRP) Actions	Completed
Detection and Analysis Phase				
1	**1.0**	**Anyone**	**Determine If an Incident Occurred**	
	1.1	Anyone	Analyze the precursors and indications. (Appendix 16-1)	
	1.2	Anyone	Look for correlating information. (Appendix 16-2)	
	1.3	Anyone	Perform research (e.g. search engines, vendor knowledge base, peer review, etc.)	
	1.4	Anyone	As soon as the incident handler believes an incident has occurred, he/she must begin documenting the incident and gathering evidence.	
2	**2.0**	**Anyone**	**Notify IT Support**	
	2.1	Anyone	The incident handler contacts IT Support and provides available documentation and evidence.	
	2.2	IT Support	IT Support classifies the incident according to Appendix 16-1	
	2.3	IT Support	If the IT Support categorizes the event as a full investigation, the IT Support technician should create a case file.	
	2.4	IT Support	IT Support on-call analyst consolidates documentation and evidence and, if applicable, stores the documentation in the case folder for the incident.	
3	**3.0**	**IT Support**	**Incident Prioritization**	
	3.1	IT Support	IT Support prioritizes handling the incident based on the business impact.	
	3.2	IT Support	IT Support will identify which IT resources have been affected and forecast which resources will be affected.	
	3.3	IT Support	IT Support will estimate the current and potential technical effect of the incident.	
4	**4.0**	**IT Support**	**Incident Notification**	
	4.1	IT Support	IT Support will contact affected asset owners and business units, alerting them to the situation.	
5	**5.0**	**Multiple Entities**	**Incident Escalation (If Required)**	
	5.1	IT Support	If the incident is believed to be significant, the IT Support technician or asset owner is responsible for notifying management for escalation.	
	5.2	Management	Management is responsible for coordinating further incident escalation steps, as required.	
Containment, Eradication, and Recovery Phase				
6	**6.0**	**IT Support**	**Secure, Document, Acquire, Preserve & Analyze Evidence (If Required)**	
	6.1	IT Support	IT Support will follow its Standard Operating Procedures (SOP) for evidence seizure and analysis.	

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.

DRP CLASSIFICATION

Information system criticality and mission importance for the DRP is the same Mission Assurance Category (MAC) levels as defined in Appendix D: Baseline Security Categorization Guidelines.

DRP SCOPING REQUIREMENTS

The DRP requirements for critical assets are summarized below:

Disaster Recovery Plan (DRP) Summary				
Criticality		MAC I	MAC II	MAC III
Data Sensitivity	Restricted	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan	High security required; must be in Disaster Recovery Plan
	Confidential	Moderate security required; must be in Disaster Recovery Plan	Moderate security required; may be in Disaster Recovery Plan	Moderate security required; need not be in Disaster Recovery Plan
	Internal Use	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal security required; need not be in Disaster Recovery Plan
	Public	Minimal security required; must be in Disaster Recovery Plan	Minimal security required; may be in Disaster Recovery Plan	Minimal security required; need not be in Disaster Recovery Plan

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.