WRITTEN INFORMATION SECURITY PROGRAM (WISP)

ACME Business Solutions, LLC

ISO 27002

Your Logo Will Be Placed Here
# Table of Contents

**WRITTEN INFORMATION SECURITY PROGRAM (WISP) OVERVIEW** 4  
**INTRODUCTION** 4  
**PURPOSE** 4  
**SCOPE & APPLICABILITY** 5  
**POLICY OVERVIEW** 5  
**VIOLATIONS** 5  
**EXCEPTIONS** 5  
**KEY TERMINOLOGY** 6  

**INFORMATION SECURITY POLICY STRUCTURE** 8  
1.0 **INFORMATION SECURITY PROGRAM POLICY** 8  
   1.1 **MANAGEMENT DIRECTION FOR INFORMATION SECURITY** 8  
   1.2 **POLICIES FOR INFORMATION SECURITY** 9  
   1.3 **REVIEW OF INFORMATION SECURITY POLICIES** 10  

**ORGANIZATION OF INFORMATION SECURITY - POLICY & STANDARDS** 11  
2.0 **INFORMATION SECURITY ORGANIZATION POLICY** 11  
   2.1 **INTERNAL ORGANIZATION** 11  
   2.2 **MOBILE DEVICES AND TELEWORKING** 15  

**HUMAN RESOURCE SECURITY - POLICY & STANDARDS** 21  
3.0 **HUMAN RESOURCE SECURITY POLICY** 21  
   3.1 **PRIOR TO EMPLOYMENT** 21  
   3.2 **DURING EMPLOYMENT** 22  
   3.3 **TERMINATION AND CHANGE OF EMPLOYMENT** 27  

**ASSET MANAGEMENT - POLICY & STANDARDS** 29  
4.0 **ASSET MANAGEMENT POLICY** 29  
   4.1 **RESPONSIBILITY FOR ASSETS** 29  
   4.2 **INFORMATION CLASSIFICATION** 33  
   4.3 **MEDIA HANDLING** 34  

**ACCESS CONTROL - POLICY & STANDARDS** 37  
5.0 **ACCESS CONTROL POLICY** 37  
   5.1 **BUSINESS REQUIREMENTS OF ACCESS CONTROL** 37  
   5.2 **USER ACCESS MANAGEMENT** 39  
   5.3 **USER RESPONSIBILITIES** 44  
   5.4 **SYSTEM AND APPLICATION ACCESS CONTROL** 45  

**ENCRYPTION - POLICY & STANDARDS** 53  
6.0 **CRYPTOGRAPHY POLICY** 53  
   6.1 **CRYPTOGRAPHIC CONTROLS** 53  

**PHYSICAL & ENVIRONMENTAL SECURITY - POLICY & STANDARDS** 57  
7.0 **PHYSICAL AND ENVIRONMENTAL SECURITY POLICY** 57  
   7.1 **SECURE AREAS** 57  
   7.2 **EQUIPMENT** 65  

**OPERATIONS SECURITY - POLICY & STANDARDS** 73  
8.0 **OPERATIONS SECURITY POLICY** 73  
   8.1 **OPERATIONAL PROCEDURES AND RESPONSIBILITIES** 73  
   8.2 **PROTECTION FROM MALWARE** 78  
   8.3 **BACKUP** 79  
   8.4 **LOGGING AND MONITORING** 82  
   8.5 **CONTROL OF OPERATIONAL SOFTWARE** 86  
   8.6 **TECHNICAL VULNERABILITY MANAGEMENT** 86  
   8.7 **INFORMATION SYSTEMS AUDIT CONSIDERATIONS** 89
COMMUNICATIONS SECURITY - POLICY & STANDARDS 91

9.0 COMMUNICATIONS SECURITY POLICY 91
  9.1 NETWORK SECURITY MANAGEMENT 91
  9.2 INFORMATION TRANSFER 95

SYSTEM ACQUISITION, DEVELOPMENT & MAINTENANCE - POLICY & STANDARDS 99

10.0 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE POLICY 99
  10.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 99
  10.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 101
  10.3 TEST DATA 107

VENDOR MANAGEMENT - POLICY & STANDARDS 109

11.0 SUPPLIER RELATIONSHIPS POLICY 109
  11.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS 109
  11.2 SUPPLIER SERVICE DELIVERY MANAGEMENT 115

INCIDENT RESPONSE - POLICY & STANDARDS 119

12.0 INFORMATION SECURITY INCIDENT MANAGEMENT POLICY 119
  12.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 119

BUSINESS CONTINUITY MANAGEMENT - POLICY & STANDARDS 124

13.0 BUSINESS CONTINUITY MANAGEMENT POLICY 124
  13.1 INFORMATION SECURITY CONTINUITY 124
  13.2 REDUNDANCIES 126

INFORMATION SECURITY COMPLIANCE - POLICY & STANDARDS 128

14.0 COMPLIANCE POLICY 128
  14.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS 128
  14.2 INFORMATION SECURITY REVIEWS 133

GLOSSARY: ACRONYMS & DEFINITIONS 135

ACRONYMS 135
DEFINITIONS 135

KEY WORD INDEX 136

RECORD OF CHANGES 137

ANNEX 1 – CYBERSECURITY POLICIES SUMMARY 138

1 - INFORMATION SECURITY PROGRAM POLICY 138
2 - INFORMATION SECURITY ORGANIZATION POLICY 138
3 - HUMAN RESOURCE SECURITY POLICY 138
4 - ASSET MANAGEMENT POLICY 138
5 - ACCESS CONTROL POLICY 138
6 - CRYPTOGRAPHY POLICY 138
7 - PHYSICAL AND ENVIRONMENTAL SECURITY POLICY 138
8 - OPERATIONS SECURITY POLICY 139
9 - COMMUNICATIONS SECURITY POLICY 139
10 - SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE POLICY 139
11 - SUPPLIER RELATIONSHIPS POLICY 139
12 - INFORMATION SECURITY INCIDENT MANAGEMENT POLICY 139
13 - BUSINESS CONTINUITY MANAGEMENT POLICY 139
14 - COMPLIANCE POLICY 139
INTRODUCTION
The Written Information Security Program (WISP) provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at ACME Business Solutions, LLC (ACME).

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

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

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

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

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

- Creating an Information Security Management System (ISMS) in accordance with ISO 27001.
- Protecting the confidentiality, integrity and availability of ACME data and information systems.
- Protecting ACME, its employees and its clients from illicit use of ACME information systems and data.
- Ensuring the effectiveness of security controls over data and information 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 Information Security risks.
- Providing for development, review and maintenance of minimum security controls required to protect ACME’s data and information systems.

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 ACME operates and safeguards its data and information 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 and procedures apply to all ACME data, information 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 and procedures 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 policies are explicitly stated for 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 not one that is less restrictive, less comprehensive, or less compliant than this policy.

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

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

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

**POLICY OVERVIEW**

In an effort to ensure an acceptable level of cybersecurity risk, ACME is required to design, implement and maintain a coherent set of policies, standards and procedures to manage risks to its data and information systems.

ACME users are required to protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and information 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 information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

**VIOLATIONS**

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

**EXCEPTIONS**

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

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that ACME uses to define common cybersecurity terms.  

Key terminology to be aware of includes:

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

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

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

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

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

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

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

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

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

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

**Information System**: A term describing an asset; a system or network that can be defined, scoped and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls and mobile devices.

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

**Policy**: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

**Procedure**: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

**Sensitive Data**: A term that covers categories of data that must be kept secure. Examples of sensitive data include Personal Data, Electronic Protected Health Information (ePHI) and all other forms of data classified as Restricted or Confidential in *Annex 1: Data Classification & Handling Guidelines*.

---

1.0 INFORMATION SECURITY PROGRAM POLICY

ACME shall protect the confidentiality, integrity and availability of its data and information 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 information system, in accordance with all legal obligations.

Management Intent: The purpose of this policy is for ACME to specify the development, implementation, assessment, authorization and monitoring of the cybersecurity program. The successful implementation of security controls depends on the successful implementation of ACME’s program-level controls.

1.1 MANAGEMENT DIRECTION FOR INFORMATION SECURITY

The objective is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations.

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 documentation is comprised of six (6) main parts:

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

![Figure 1.1: Cybersecurity Documentation Hierarchy](image)

---

3 ISO/IEC 27002:2013 – 5.1
1.2 Policies for Information Security
A set of policies for cybersecurity should be defined, approved by management, published and communicated to employees and relevant external parties. 4

1.2.1 Publishing an Information Security Policy
Control Objective: The organization establishes, publishes, maintains and disseminates a security policy. 5

Standard: ACME’s cybersecurity policies and standards shall be represented in a single document, the Written Information Security Program (WISP) that shall be:
(a) Endorsed by executive management; and
(b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

Supplemental Guidance: A company’s cybersecurity policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

1.2.2 Information Security Program Plan
Control Objective: The organization: 6

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

Standard: ACME’s cybersecurity policies and standards shall be represented in a single document, the Written Information Security Program (WISP) that:
(a) Shall be reviewed and updated at least annually; and
(b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

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

1.2.3 Assigned Information Security Responsibilities
Control Objective: The organization appoints an individual assigned with the mission and resources to coordinate, develop, implement and maintain an organization-wide cybersecurity program. 7

Standard: The authority and responsibility for managing the cybersecurity program are delegated to ACME’s Information Security Officer (ISO) and he/she is required to perform or delegate the following cybersecurity management responsibilities:
(a) Establish, document and distribute security policies and procedures;
(b) Monitor and analyze security alerts and information;
(c) Distribute and escalate security alerts to appropriate personnel;
(d) Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
(e) Administer user accounts, including additions, deletions and modifications; and

---

4 ISO/IEC 27002:2013 – 5.1.1
5 NY DFS 500.03
6 HIPAA 164.308(a)(1)(i) & 164.316(a)-(b) | GLBA Sec 6801(b)(1) | PCI DSS v3.2 12.1 & 12.1.1 | MA201CMR17 17.03(1), 17.04 & 17.03(2)(b)(2) | NIST CSF v1.1 ID.GV-1 & ID.GV-2 | NY DFS 500.02
7 HIPAA 164.308(a)(2) | GLBA Safeguards Rule | PCI DSS v3.2 12.5-12.5.5 | MA201CMR17 17.03(2)(a) | OR646A.622(2)(d)(A)(i) | NIST CSF v1.1 ID.AM-6 & ID.GV-2 | NY DFS 500.04
Supplemental Guidance: None

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

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

Supplemental Guidance: None

1.2.5 RISK MANAGEMENT
Control Objective: The organization implements a risk-assessment process. 8

Standard: Asset custodians are required to implement a risk-assessment process that:
(a) Is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Identifies critical assets, threats and vulnerabilities; and
(c) Results in a formal risk assessment.

Supplemental Guidance: Examples of risk assessment methodologies include but are not limited to
- OCTAVE;
- ISO 27005; and
- NIST SP 800-30.

1.3 REVIEW OF INFORMATION SECURITY POLICIES
The policies for cybersecurity should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. 9

1.3.1 INFORMATION SECURITY DOCUMENTATION REVIEW
Control Objective: The organization reviews its cybersecurity policies, standards and procedures at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. 10

Standard: At least annually, or as business needs exist, the Written Information Security Program (WISP) will be reviewed for applicability and updated accordingly.

Supplemental Guidance: Updates to the 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.

---

8 PCI DSS v3.2 12.2 | NY DFS 500.09 | NIST CSF v1.1 ID.GV-4, ID.RM-1, ID.RM-2, ID.RM-3, PR.IP-7 & PR.IP-8
9 ISO/IEC 27002:2013 – 5.1.2 | NIST CSF v1.1 PR.IP-7 & PR.IP-8
10 | NY DFS 500.03
3.0 HUMAN RESOURCE SECURITY POLICY
ACME shall ensure cybersecurity best practices are incorporated into Human Resources (HR) personnel management practices.

Management Intent: The purpose of this policy is to ensure Human Resources (HR) personnel management incorporates cybersecurity best practices.

3.1 PRIOR TO EMPLOYMENT
The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

3.1.1 SCREENING
Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

3.1.1.1 PERSONNEL SCREENING
Control Objective: The organization:
- Screens individuals prior to authorizing access to the information system; and
- Rescreens individuals, if necessary, based on organizational concerns.

Standard: ACME’s Human Resources (HR) department is responsible for screening potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources.

Supplemental Guidance: Approved methods of screening procedures include:
- Previous employment history verification;
- Criminal history record check;
- Department of Motor Vehicles (DMV) history check;
- Credit history; and
- Personal/professional reference checks.

3.1.2 TERMS AND CONDITIONS OF EMPLOYMENT
The contractual agreements with employees and contractors should state their and the organization’s responsibilities for cybersecurity.

3.1.2.1 ACCESS AGREEMENTS
Control Objective: The organization:
- Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and
- Reviews/updates the access agreements.

Standard: ACME is required to ensure that access to information with special protection measures is granted only to individuals who:
   (a) Have a valid access authorization; and
   (b) Satisfy associated personnel security criteria.

---

31 ISO/IEC 27002:2013 – 7.1
32 ISO/IEC 27002:2013 – 7.1.1
33 HIPAA 164.308(a)(3)(ii) & (B) | PCI DSS v3.2 12.7 | NIST CSF v1.1 PR.DS-5 & PR.IP-11
34 ISO/IEC 27002:2013 – 7.1.2
35 HIPAA 164.308(a)(4)(i) | NIST CSF v1.1 PR.DS-5 & PR.IP-11
Supplemental Guidance: Prior to granting any access to ACME information systems or data, a Non-Disclosure Agreement (NDA) should be signed by the employee, contractor, service provider or partner requiring access. This NDA should be maintained on file in accordance with document retention guidelines.

3.2 DURING EMPLOYMENT
The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

3.2.1 MANAGEMENT RESPONSIBILITIES
Management should require all employees and contractors to apply cybersecurity in accordance with the established policies and procedures of the organization.

3.2.1.1 RULES OF BEHAVIOR
Control Objective: The organization:

- Develops usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.
- Verifies that the usage policies require acceptable uses for the technology.
- Verifies that the usage policies require acceptable network locations for the technology.
- Prohibits copy, move and storage of sensitive data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need; and
- Establishes end-user messaging technologies restrictions.

Standard: ACME’s Human Resources (HR) department is responsible for developing usage policies for technologies and defining proper use of these technologies, ensuring:

(a) Information systems can only be used after explicit approval is given by company management;
(b) User authentication must be enabled, when technically feasible;
(c) Acceptable uses of the technologies must be given; and
(d) Acceptable network locations must be clearly stated.

Supplemental Guidance: An investigation should take place when there is:

- A credible allegation or evidence of unethical or unlawful acts, fraud or gross misconduct, including but not limited to acts which could reasonably form the basis of a claim against ACME for unlawful discrimination, harassment or retaliation; or
- A requirement to do so by law, regulation or policy.

Where law enforcement becomes involved in the subject of an internal investigation, ACME needs to be prepared to cooperate with authorities consistent with its legal obligations to employees.

3.2.1.2 SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS
Control Objective: The organization includes in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing information system account information.

Standard: ACME’s Human Resources (HR) department is responsible for developing usage policies and guidance specifically for social media and social networking usage.

Supplemental Guidance: This control enhancement addresses rules of behavior related to use of social media and networking sites:

- When using such media and sites for official duties;
- When organizational information is involved in the social media/networking transactions; and
- When accessing social media/networking sites from organizational information systems.
7.0 PHYSICAL AND ENVIRONMENTAL SECURITY POLICY
ACME shall ensure physical access controls are in place to limit physical access to authorized personnel and provide appropriate environmental controls to protect both data and information systems from environmental hazards.

Management Intent: The purpose of this policy is to minimize risk to ACME information systems and data by addressing applicable physical security and environmental concerns.

7.1 SECURE AREAS
The objective is to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.\(^{138}\)

7.1.1 PHYSICAL SECURITY PERIMETER
Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.\(^{139}\)

7.1.1.1 PHYSICAL ACCESS AUTHORIZATIONS
Control Objective: The organization:\(^{140}\)

- Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
- Issues authorization credentials; and
- Reviews and approves the access list and removes from the access list personnel no longer requiring access.

Standard: ACME is required to:

(a) Develop and keeps current a list of personnel with authorized access to its facilities, except for those areas within the facility officially designated as publicly accessible;
(b) Issue authorization credentials for physical access; and
(c) Review and approve the access list and remove from the access list personnel no longer requiring access.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards and smart cards. Organizations determine the strength of authorization credentials needed (including the level of forge-proof badges, smart cards, or identification cards) consistent with standards, policies and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

7.1.1.2 ROLE-BASED PHYSICAL ACCESS
Control Objective: The organization authorizes physical access to the facility where the information system resides, based on the position or role of a user.\(^{141}\)

Standard: ACME is required to authorize physical access to its facilities based on position or role.

Supplemental Guidance: ACME should restrict physical access to information systems that process sensitive information to authorized personnel with the appropriate roles and access authorizations. Roles for physical access include, but are not limited to:

- Employees
- Contractors
- Vendors
- Partners
- Guests
- Maintenance Personnel

\(^{138}\) ISO/IEC 27002:2013 – 11.1
\(^{139}\) ISO/IEC 27002:2013 – 11.1.1
\(^{140}\) HIPAA 164.310(a)(2)(ii) \| PCI DSS v3.2.2 9.2 \| NIST CSF v1.1 PR.AC-2
\(^{141}\) HIPAA 164.310(a)(2)(iii)
7.1.1.3 Identification Requirement

Control Objective: The organization requires at least one form of government-issued photo identification to gain access to the facility where the information system resides.  

Standard: ACME requires at least one (1) form of government-issued photo identification to gain access.

Supplemental Guidance: Acceptable forms of government photo identification include, for example:
- Passports;
- Personal Identity Verification (PIV) cards; and
- Drivers’ licenses.

In the case of gaining access to facilities using automated mechanisms, organizations may use personal identity verification cards, key cards, PINs and biometrics.

7.1.1.4 Restrict Unescorted Access

Control Objective: The organization restricts unescorted access to the facility where the information system resides to personnel with required security clearances, formal access authorizations and validated the need for access.

Standard: ACME is required to restrict physical access to the information systems equipment and records storage.

Supplemental Guidance: None

7.1.1.5 Physical Access Control

Control Objective: The organization:

- Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
- Verifies individual access authorizations before granting access to the facility;
- Controls entry to the facility containing the information system using physical access devices and/or guards;
- Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk;
- Secures keys, combinations and other physical access devices; and
- Changes combinations and keys and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Standard: ACME is required to:

(a) Use video cameras and/or access control mechanisms to limit and monitor physical access to the facility and information systems;
(b) Enforce physical access authorizations for all physical access points (including designated entry/exit points) to company-owned or operated facilities;
(c) Verify individual access authorizations before granting access to the facility;
(d) Control access to areas based on the physical security zone requirements;
(e) Secure keys, combinations and other physical access devices; and
(f) Change combinations and keys and when keys are lost, when combinations are compromised, or when individuals are transferred or terminated.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations and card readers. Safeguards for

---

142 PCI DSS v3.2 9.4 & 9.4.1  
143 PCI DSS v3.2 9.3  
144 HIPAA 164.310(a)(2)(iv) | PCI DSS v3.2 9.1, 9.1.1, 9.1.2 & 9.2 | MA201CMR17 17.03(2)(g) | OR646A.622(2)(d)(C)(ii) | NIST CSF v1.1 PR.AC-2, DE.CM-2, DE.CM-7 & DE.DP-3
publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, isolating selected information systems/components in secured areas. Components of information systems (e.g., workstations, computer terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

**7.1.1.6 PHYSICAL ACCESS LOGS**

Control Objective: The physical access control system generates a log entry for each access.

**Standard:** ACME is required to configure access control systems to log the following information:

(a) Physical location of the access;
(b) Direction of access, if possible (e.g., ingress or egress);
(c) Identity of the person accessing the location; and
(d) Indication of success or failure.

**Supplemental Guidance:** Access control systems include card / badge readers and keypad readers.

**7.1.1.7 LOCKABLE PHYSICAL CASINGS**

Control Objective: The organization uses lockable physical casings to protect organization-defined information system components from unauthorized physical access.

**Standard:** ACME is required to protect sensitive information systems from physical tampering or alteration of hardware components by utilizing lockable physical casings.

**Supplemental Guidance:** Lockable physical casings are primarily associated with rack-mounted hardware.

**7.1.1.8 ACCESS CONTROL FOR TRANSMISSION MEDIUM**

Control Objective: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

**Standard:** ACME management is required to limit physical access to transmission medium to only authorized personnel.

**Supplemental Guidance:** Physical security safeguards applied to information system distribution and transmission lines help prevent accidental damage, disruption and physical tampering. Transmission medium includes but are not limited to:

- Publicly accessible network jacks;
- Wireless Access Points (WAPs);
- Border protection devices (including firewalls & routers);
- Networking/communications hardware; and
- Telecommunication lines.

Protective measures to control physical access to information system distribution and transmission lines include:

- Locked wiring closets;
- Disconnected or locked spare jacks; and
- Protection of cabling by conduit or cable trays.

**7.1.1.9 ACCESS CONTROL FOR OUTPUT DEVICES**

Control Objective: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Standard:** Physical access to information system output devices must be limited to authorized personnel to prevent unauthorized individuals from obtaining access to unsecured data.

---

145 PCI DSS v3.2 9.1.2 & 9.1.3 | OR646A.622(2)(d)(C)(ii) | NIST CSF v1.1 PR.AC-2
146 OR646A.622(2)(d)(C)(ii) | NIST CSF v1.1 PR.AC-2
- SUPPLEMENTAL DOCUMENTATION -

WRITTEN INFORMATION SECURITY PROGRAM (WISP)

ANNEXES, TEMPLATES & REFERENCES

Version 2020.1
# Table of Contents

## Annexes
- Annex 1: Data Classification & Handling Guidelines 3
- Annex 2: Data Classification Examples 8
- Annex 3: Data Retention Periods 10
- Annex 4: Baseline Security Categorization Guidelines 12
- Annex 5: Rules of Behavior (Acceptable & Unacceptable Use) 14
- Annex 6: Guidelines for Personal Use of Organizational IT Resources 16
- Annex 7: Risk Management Framework (RMF) 17
- Annex 8: System Hardening 20

## Templates
- Template 1: Management Directive (Policy Authorization) 22
- Template 2: User Acknowledgement Form 23
- Template 3: User Equipment Receipt of Issue 24
- Template 4: Service Provider Non-Disclosure Agreement (NDA) 25
- Template 5: Incident Response Plan (IRP) 26
- Template 6: Incident Response Form 37
- Template 7: Appointment Orders (Information Security Officer) 38
- Template 8: Privileged User Account Request Form 39
- Template 9: Change Management Request Form 40
- Template 10: Change Control Board (CCB) Meeting Minutes 42
- Template 11: Plan of Action & Milestones (POA&M) / Risk Register 43
- Template 12: Ports, Protocols & Services (PPS) 44
- Template 13: Business Impact Analysis (BIA) 45
- Template 14: Disaster Recovery Plan (DRP) & Business Continuity Plan (BCP) 47
- Template 15: Privacy Impact Assessment (PIA) 51

## References
- Reference 1: WISP Exception Request Process 53
- Reference 2: Electronic Discovery (eDiscovery) Guidelines 54
- Reference 3: Types of Security Controls 55
- Reference 4: Information Security Management System (ISMS) 56
### ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

**DATA CLASSIFICATION**

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

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

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

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

GENERAL ASSUMPTIONS

- Any information created or received by ACME employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.

- Treat information that is not assigned a classification level as “Internal Use” at a minimum and use corresponding controls.

- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.

- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.

- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

PERSONAL DATA (PD)
PD is any information about an individual maintained by ACME including any information that:

- Can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and

- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

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

- **Name**
  - Full name;
  - Maiden name;
  - Mother’s maiden name; and
  - Alias(es);

- **Personal Identification Numbers**
  - Social Security Number (SSN);
  - Passport number;
  - Driver’s license number;
  - Taxpayer Identification Number (TIN), and
  - Financial account or credit card number;

- **Address Information**
  - Home address; and
  - Personal email address;

- **Personal Characteristics**
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting, and
### Data Handling Guidelines

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

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

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

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Sensitive Data Elements</th>
<th>Public</th>
<th>Internal Use</th>
<th>Confidential</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client or Employee Personal Data</td>
<td>Social Security Number (SSN)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employer Identification Number (EIN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Driver’s License (DL) Number</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Account Number</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Payment Card Number (credit or debit)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Government-Issued Identification (e.g., passport, permanent resident card, etc.)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controlled Unclassified Information (CUI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Birth Date</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>First &amp; Last Name</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Age</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone and/or Fax Number</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Address</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethnicity</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Address</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Employee-Related Data</td>
<td>Compensation &amp; Benefits Data</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical Data</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workers Compensation Claim Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Education Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dependent or Beneficiary Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sales &amp; Marketing Data</td>
<td>Business Plan (including marketing strategy)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Data Related to Revenue Generation</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marketing Promotions Development</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>News Releases</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking &amp; Infrastructure Data</td>
<td>Username &amp; Password Pairs</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public Key Infrastructure (PKI) Cryptographic Keys (public &amp; private)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware or Software Tokens (multifactor authentication)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Configuration Settings</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regulatory Compliance Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal IP Addresses</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privileged Account Usernames</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Provider Account Numbers</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Strategic Financial Data</td>
<td>Corporate Tax Return Information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal Billings</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Budget-Related Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unannounced Merger and Acquisition Information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trade Secrets (e.g., design diagrams, competitive information, etc.)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Operating Financial Data</td>
<td>Electronic Payment Information (Wire Payment / ACH)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paychecks</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incentives or Bonuses (amounts or percentages)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stock Dividend Information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bank Account Information</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
### ANNEX 3: DATA RETENTION PERIODS

The following schedule highlights suggested retention periods* for some of the major categories of data:

*Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, contract, filing, etc.)*

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TYPE OF RECORD</th>
<th>RETENTION PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business</strong></td>
<td>Amendment</td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Records</strong></td>
<td>Annual Reports</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Articles of Incorporation</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Board of Directors (elections, minutes, committees, etc.)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Bylaws</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Capital stock &amp; bond records</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Charter</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Contracts &amp; agreements</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Copyrights</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Correspondence (General)</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Correspondence (Legal)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Partnership agreement</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Patents</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Service marks</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Stock transfers</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Trademarks</td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Audit report (external)</td>
<td>Permanent</td>
</tr>
<tr>
<td><strong>Records</strong></td>
<td>Audit report (internal)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Balance sheets</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Bank deposit slips, reconciliations &amp; statements</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Bills of lading</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Budgets</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Cash disbursement &amp; receipt record</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Checks (canceled)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Credit memos</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Depreciation schedule</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Dividend register &amp; canceled dividend checks</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Employee expense reports</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Employee payroll records (W-2, W-4, annual earnings records, etc.)</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Financial statements (annual)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Freight bills</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>General ledger</td>
<td>Persistent</td>
</tr>
<tr>
<td></td>
<td>Internal reports (work orders, sales reports, production reports)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Inventory lists</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Investments (sales &amp; purchases)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Profit / Loss statements</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Purchase and sales contracts</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Purchase order</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Subsidiary ledgers (accounts receivable, accounts payable, etc.)</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Tax returns</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Vendor Invoices</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Worthless securities</td>
<td>7</td>
</tr>
</tbody>
</table>
ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL).*

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

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

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

![Asset Categorization Matrix]

**Figure 1: Asset Categorization Risk Matrix**

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

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

**RISK MANAGEMENT OVERVIEW**

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

![Risk Management Diagram]

**Figure 1: Risk Overview**

**RISK MANAGEMENT FRAMEWORK (RMF)**

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

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

**PLAN OBJECTIVES**

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

**INCIDENT DISCOVERY**

<table>
<thead>
<tr>
<th>Malicious Actions</th>
<th>Possible Indications of an Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service (DoS) Examples</td>
<td>You might be experiencing a DoS if you see…</td>
</tr>
</tbody>
</table>
| Network-based DoS against a particular host | • User reports of system unavailability  
• Unexplained connection losses  
• Network intrusion detection alerts  
• Host intrusion detection alerts (until the host is overwhelmed)  
• Increased network bandwidth utilization  
• Large number of connections to a single host  
• Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host)  
• Firewall and router log entries  
• Packets with unusual source addresses                                                                 |
**DISASTER RECOVERY PLAN (DRP)**

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

**RDP CLASSIFICATION**

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

**DRP SCOPING REQUIREMENTS**

The DRP requirements for critical assets are summarized below:

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

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

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

**DATA BACKUP AVAILABILITY**

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