Your Logo
Will Be
Placed Here

DIGITAL SECURITY PROGRAM (DSP)

ACME Business Consulting, LLC

DSP
Digital Security Program

Table of Contents

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Business Consulting, LLC (ACME)'s systems, applications and services to protect its data, regardless of where it is stored, transmitted or processed. The following external content is a non-exhaustive list of frameworks that either support the implementation of or are referenced by the Digital Security Program (DSP):

- The National Institute of Standards and Technology (**NIST**): [1]
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-64: *Security Considerations in Secure Development Life Cycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personal Data (PD)*
  - NIST SP 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- The International Organization for Standardization (**ISO**):[2]
  - ISO/IEC 15288: *Systems and Software Engineering -- System Life Cycle Processes*
  - ISO/IEC 22301: *Societal Security – Business Continuity Management Systems – Requirements*
  - ISO/IEC 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
  - ISO/IEC 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personal Data (PD) in Public Clouds Acting as PD Processors*
  - ISO/IEC 27701: *Information Technology - Security Techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines*
- Other influencing frameworks (alphabetical order):
  - AuditScripts. *Open Threat Taxonomy*[3]
  - Center for Internet Security (**CIS**) Critical Security Controls (**CSC**)[4]
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[5]
  - Control Objectives for Information and Related Technologies (**COBIT**)[6]
  - Defense Information Systems Agency (**DISA**) Secure Technology Implementation Guides (**STIGs**)[7]
  - Department of Defense Cybersecurity Maturity Model Certification (**CMMC**)[8]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[9]
  - Fair Information Practice Principles (**FIPP**)[10]
  - Generally Accepted Privacy Practices (**GAPP**)[11]
  - Open Web Application Security Project (**OWASP**)[12]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[13]
  - Privacy by Design (**PbD**) [14]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf
[4] Center for Internet Security - https://www.cisecurity.org/
[5] Cloud Security Alliance - https://cloudsecurityalliance.org/
[6] COBIT - http://www.isaca.org/COBIT/Pages/default.aspx
[7] DoD Information Security Agency - https://public.cyber.mil/
[8] DoD Cybersecurity Maturity Model Certification - https://www.acq.osd.mil/cmmc/index.html
[9] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[10] Federal Trade Commission - https://www.ftc.gov
[11] The American Institute of CPAs - http://www.aicpa.org
[12] OWASP - https://www.owasp.org/index.php/Main_Page
[13] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/
[14] Term and principles coined by Dr. Ann Cavoukian - https://www.owasp.org/index.php/Privacy_by_Design

INTRODUCTION

The Digital Security Program (DSP) provides definitive information on the prescribed measures used to establish and enforce the security program at ACME Business Consulting, LLC (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 data and the systems that collect, process and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:

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

Commensurate with risk, security 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.

PURPOSE

The purpose of the Digital Security Program (DSP) is to prescribe a comprehensive framework for:

- Creating a leading practice-based Information Security Management System (ISMS);
- Protecting the confidentiality, integrity, availability and safety 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 control objectives, 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 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 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 standards. ACME departments shall use these standards or may create a more restrictive standard, but none that are less restrictive, less comprehensive or less compliant than these standards.

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

ACME's documented roles and responsibilities provides a detailed description of ACME user roles and responsibilities, in regards to cybersecurity-related use obligations.

ACME reserves the right to revoke, change or supplement these policies, standards 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.

The DSP addresses the policies, standards and guidelines. Data / process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with DSP requirements.

ACME users are required to protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) 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 of Policies, Standards and/or Procedures

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.

Exception To Standards

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

Updates To Policies & Standards

Updates to the Digital Security Program (DSP) will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that ACME uses to define common cybersecurity terms.[15] Key terminology to be aware of includes:

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a ACME owns or controls.

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

Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for Software-as-a-Service (Saas), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

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 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 diligence and due care requirements.

Cybersecurity / 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, Availability and Safety (CIAS) of data.

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 Controller. A term describing the privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing Personal Data (PD) other than natural persons who use data for personal purposes

Data Principle. A term describing the natural person to whom the Personal Data (PD) relates

Data Processor. A term describing the privacy stakeholder that processes Personal Data (PD) on behalf of and in accordance with the instructions of a PD controller

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 Technology (IT). A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

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.

[15] NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf

Personal Data / Personal Information (PD). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[16]

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.

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

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

Sensitive Personal Data (sPD) / Sensitive Personal Information (sPI): A term describing personal data, revealing:

- The first name or first initial and last name, in combination with any one or more of the following data elements: [17]
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN);
  - Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.);
  - Financial account number; or
  - Payment card number (e.g., credit or debit card);
- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade-union membership;
- Physical or mental health;
- Sex life and sexual orientation;
- Genetic data; and / or
- Biometric data.[18]

Standard: A term describing formally established requirements in regard to processes, actions and configurations.

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.

Target Audience: A term describing the intended group for which a control or standard is directed.

[16] European Union General Data Protection Requirement – Article 4(1)
[17] The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
[18] European Union General Data Protection Requirement – Article 9(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. [19]

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-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 leading practices, 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.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Information security 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.

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.

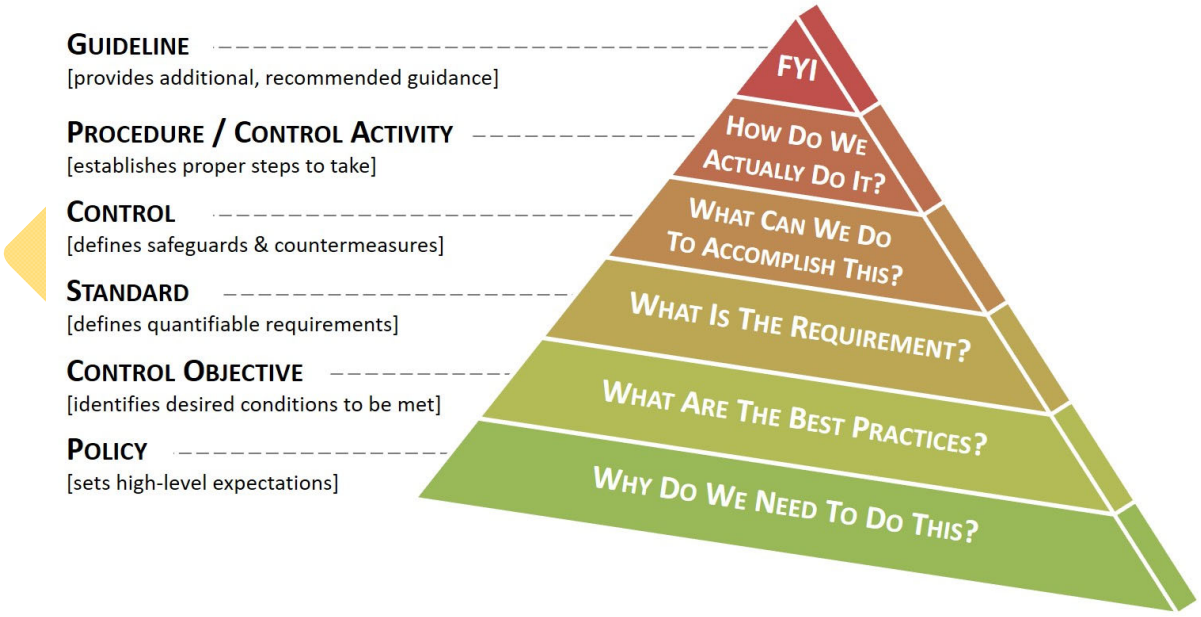

Figure 1: Information Security Documentation Framework

[19] ISO 27002:2013 5.1

Management Intent: The purpose of the Security & Privacy Governance (GOV) policy is to specify the development, proactive management and ongoing review of ACME's security and privacy program.

Policy: ACME shall protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored. Digital 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, in accordance with all statutory, regulatory and contractual obligations.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide digital security policy, as well as associated standards, controls and procedures. [20]

Standard: ACME's security program shall be represented in a single document, the Digital Security Program (DSP) 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.

Guidelines: The security plans for individual systems and the organization-wide DSP together provide complete coverage for all cybersecurity and privacy-related controls employed within the organization.

GOV-02: PUBLISHING SECURITY & PRIVACY POLICIES

Control Objective: The organization establishes, publishes, maintains and disseminates security and privacy policies. [21]

Standard: ACME's security and privacy policies and standards shall be represented in a consolidated document, the Digital Security Program (DSP) that shall be:

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

Guidelines: An organization's cybersecurity policies create the roadmap for implementing cybersecurity and privacy measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

GOV-03: PERIODIC REVIEW & UPDATE OF SECURITY & PRIVACY DOCUMENTATION

Control Objective: The organization reviews its security and privacy policies, standards and procedures at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. [22]

Standard: ACME's business leadership (or other accountable business role or function) shall review the Digital Security Program (DSP) at planned intervals or as a result of changes to the organization (e.g., mergers, acquisitions, partnerships, new products, etc.) to ensure its continuing alignment with the security strategy, risk posture, effectiveness, accuracy, relevance and applicability to statutory, regulatory and / or contractual compliance obligations.

Guidelines: Updates to the DSP 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.

[20] NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.1
[21] NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.1 | NIST CSF v1.1 ID.GV-1
[22] NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.2

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

Policy: All technology changes to production environments must follow a standard process to reduce the risk associated with change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide change management policy, as well as associated standards, controls and procedures. [84]

Standard: Data/process owners and asset custodians are required to test, validate and document changes to systems before implementing the changes on the production network.

Guidelines: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality or privacy or any combination thereof.

CHG-02: CONFIGURATION CHANGE CONTROL

Control Objective: The organization follows change control processes and procedures for all changes to system components. The organization:[85]

- Determines the types of changes to systems that are configuration controlled;
- Approves configuration-controlled changes to systems with explicit consideration for security impact analyses;
- Documents approved configuration-controlled changes to systems;
- Retains and reviews records of configuration-controlled changes to systems;
- Audits activities associated with configuration-controlled changes to systems; and
- Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes on a routine basis.

Standard: Data/process owners and asset custodians are required to follow change control processes and procedures for all changes to system components:

(a) Utilize separate environments for development / testing / staging and production;
(b) Utilize a separation of duties between development / testing / staging and production environments;
(c) Prohibit the use of production data (e.g., live PANs) for testing or development;
(d) Remove test data and accounts before production systems become active / goes into production; and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following:
    1. Documentation of impact;
    2. Documented change approval by authorized parties;
    3. Functionality testing to verify that the change does not adversely impact the security of the system; and
(f) Back-out procedures.
(g) Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed systems and networks and documentation updated as applicable.

Guidelines: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review and disposition of changes to the systems, including system upgrades and modifications. Configuration change

[84] NIST 800-53 rev4 CM-3 | ISO 27002:2013 12.1.2
[85] NIST 800-53 rev4 CM-3 | ISO 27002:2013 14.2.2 | NIST 800-171 rev1 3.4.3 | NIST CSF v1.1 PR.IP-3

control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers and mobile devices), unscheduled / unauthorized changes and changes to remediate vulnerabilities.

CHG-02(A): CONFIGURATION CHANGE CONTROL | PROHIBITION OF CHANGES

Control Objective: The organization prohibits changes to systems until designated approvals are received.[86]

Standard: Data/process owners and asset custodians are prohibited from implementing a change without first obtaining Pre-approval from the Change Control Board (CCB) and notifying all affected parties prior to the implementation of the change.

Guidelines: The scope of affected parties must include any clients, partners or vendors that would be affected by the change.

CHG-02(B): CONFIGURATION CHANGE CONTROL | TEST, VALIDATE & DOCUMENT CHANGES

Control Objective: The organization tests, validates and documents changes in a non-production environment before changes are implemented in a production environment.[87]

Standard: Where technically feasible, asset custodians and data / process owners are required to test and validate configuration changes in a test environment, prior to deploying the change in the production environment.

Guidelines: When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. If it is not technically or logistically feasible to test a configuration change, compensating control should be identified and implemented in order to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include, but is not limited to:

- Images of systems;
- Backups of configurations;
- Viable back out plan;
- After-hours implementation; and
- Pilot / test group rollouts.

CHG-02(C): CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE FOR CHANGE

Control Objective: The organization includes a cybersecurity representative in the configuration change control review process.[88]

Standard: ACME's cybersecurity personnel are required to represent cybersecurity topics as a representative of ACME's Change Control Board (CCB).

Guidelines: Information security representatives can include, for example, system security officers or system security managers.

CHG-02(D): CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

Control Objective: The information system implements organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner. [89]

Standard: Where technically feasible and justified by a valid business case, ACME shall:

(a) Employ automated mechanisms that remediate non-conforming systems to ACME-approved baseline configurations; and
(b) Alert incident response personnel to the possible security incident that generated the need to revert the configuration.

Guidelines: Security responses include, for example, halting information system processing, halting selected system functions or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item.

CHG-02(E): CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHIC MANAGEMENT

Control Objective: The organization ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management. [90]

[86] NIST 800-53 rev4 CM-3(1)
[87] NIST 800-53 rev4 CM-3(2) | ISO 27002:2013 14.2.3
[88] NIST 800-53 rev4 CM-3(5)
[89] NIST 800-53 rev4 CM-3(4)
[90] NIST 800-53 rev4 CM-3(6)

Management Intent: The purpose of the Data Classification & Handling (DCH) policy is to ensure that technology assets are properly classified and measures are implemented to protect ACME's data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity and availability of data.

Policy: In accordance with all applicable legal requirements, ACME shall protect data in both hardcopy and digital form by limiting access to authorized users and utilize methods of sanitizing or destroying media so that data recovery is technically infeasible.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

DCH-01: DATA PROTECTION

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide data protection policy, as well as associated standards, controls and procedures. [202]

Standard: Data/process owners and asset custodians must:

(a) In accordance with all applicable statutory, regulatory and contractual compliance obligations, implement and govern controls to protect ACME data wherever it is stored, transmitted and processed;
(b) Define retention periods for both sensitive and non-sensitive data;
(c) Dispose of, destroy, erase and / or anonymizes data once it is no longer necessary for business purposes;
(d) Maintain strict control over the storage and accessibility of media; and
(e) Maintain inventories of sensitive data under their control.

Guidelines: The objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.

DCH-01(A): DATA PROTECTION | DATA STEWARDSHIP

Control Objective: The organization designates data with individual stewardship by assigned responsibilities that are defined, documented and communicated.

Standard: At least annually, data / process owner is required to assess the following criteria, as it pertains to their data and / or processes:

(a) Data classification requirements;
(b) System criticality;
(c) Geographical storage and / or processing of the data; and
(d) Applicable statutory, regulatory and contractual requirements.

Guidelines: A complete inventory of business-critical assets located at all sites and / or geographical locations and their usage over time should be maintained and updated regularly and assigned ownership by defined roles and responsibilities.

DCH-02: DATA & ASSET CLASSIFICATION

Control Objective: The organization: [203]

- 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: Assets must be classified in terms of system criticality and data sensitivity (see *Annex 4: Baseline Security Categorization Guidelines*). Data/process owners and asset custodians are required to:

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

[202] NIST 800-53 rev4 AR-7, DM-2, DM-2(b) & MP-1 | ISO 27002:2013 8.2, 8.3.3 & 18.1.4
[203] ISO 27002:2013 8.2.1 | NIST CSF v1.1 ID.AM-5

Guidelines: 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.

DCH-03: Media Access

Control Objective: The organization restricts access to types of digital and non-digital media to authorized individuals using organization-defined security measures.[204]

Standard: Data/process owners and asset custodians are required to restrict access to digital and non-digital media to authorized individuals.

Guidelines: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external / removable hard drives, flash drives, compact disks and digital video disks. Non-digital media includes, for example, paper and microfilm. For media containing information determined by organizations to be in the public domain, to be publicly releasable or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls may provide adequate protection.

DCH-03(A): Media Access | Disclosure of Information

Control Objective: The organization limits the disclosure of information to authorized parties.

Standard: ACME personnel, including ACME subcontractors, are prohibited from releasing any information, regardless of medium (e.g., voice, email, film, tape, document, etc.), pertaining to any part of a contract, project or program to anyone outside of ACME. The only exceptions are if:

(a) The project's contracting officer has given prior written approval; or
(b) The information is otherwise in the public domain before the date of release.

Guidelines: None

DCH-03(B): Media Access | Masking Displayed Data

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

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), where no more than the first six (6) / last four (4) digits are allowed to be shown.

Guidelines: Only personnel with a legitimate business need should be able to see more than the first six (6) / last four (4) of the PAN.

DCH-04: Media Marking

Control Objective: The organization marks media in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats and applicable security requirements.[205]

Standard: ACME users are required to mark media in accordance with ACME's Data & Asset Classification Standard.

Guidelines: Reference *Annex 1: Data Classification & Handling Guidelines* for examples of data classification and handling.

The term security marking refers to the application / use of human-readable security attributes. The term security labeling refers to the application / use of security attributes with regard to internal data structures within systems. System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external / removable hard drives, flash drives,

[204] NIST 800-53 rev4 MP-2 & MP-2(1) | NIST 800-171 rev1 3.8.1, 3.8.2 & 3.8.3
[205] NIST 800-53 rev4 MP-3 | ISO 27002:2013 8.2.2 | NIST 800-171 rev1 3.8.4

Standard: Where technically feasible and justified by a valid business case, ACME shall employ an automatic fire suppression capability in its data center environments where sensitive data and/or critical systems are located.

Guidelines: None

PES-09: Temperature & Humidity Controls

Control Objective: The organization:[508]

- Maintains temperature and humidity levels within the facility; and
- Monitors temperature and humidity levels.

Standard: In data center environments, asset custodians are required to employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Guidelines: Temperature and humidity controls typically apply to facilities containing concentrations of system resources, for example, data centers, server rooms and mainframe computer rooms.

PES-09(A): Temperature & Humidity Controls | Monitoring with Alarms / Notifications

Control Objective: The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.[509]

Standard: Where technically feasible, ACME shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Guidelines: None

PES-10: Delivery & Removal

Control Objective: The organization uses controlled access points to isolate information processing facilities for points, such as delivery and loading areas, to avoid unauthorized access.[510]

Standard: Systems are prohibited from being removed from ACME facilities without prior, management authorization. Prior to the removal of the system, the following information needs to be captured:

(a) Make / model / serial # of the asset;
(b) Owner of the asset;
(c) Reason the asset is being removed from the facility;
(d) Company and name of representative removing the asset; and
(e) Estimated return date for the asset, if applicable.

Guidelines: Effectively enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and possibly isolating the areas from the system and media libraries.

PES-11: Alternate Work Site

Control Objective: The organization:[511]

- Employs organization-defined management, operational and technical system security controls at alternate work sites;
- Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- Provides a means for employees to communicate with cybersecurity personnel in case of security incidents or problems.

Standard: ACME management is required to develop plans regarding alternate work sites that include:

(a) System security controls at alternate work sites;
(b) The effectiveness of security controls at alternate work sites; and

[508] NIST 800-53 rev4 PE-14 |
[509] NIST 800-53 rev4 PE-14(2)
[510] NIST 800-53 rev4 PE-16 | ISO 27002:2013 11.1.6
[511] NIST 800-53 rev4 PE-17 | NIST 800-171 rev1 3.10.6

PRI-06: DATA SUBJECT ACCESS

Control Objective: The organization provides individuals with access to their personal information for review and update.[530]

Standard: ACME must implement mechanisms to grant identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to the data subject consistent with the entity's privacy commitments and system requirements. If access is denied, the data subject must be informed of the denial and reason for such denial, as required, consistent with ACME's privacy commitments and system requirements.

Guidelines: 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.

PRI-06(A): DATA SUBJECT ACCESS | REDRESS INACCURATE INFORMATION

Control Objective: The organization establishes and implements a process for: [531]

- Individuals to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and
- Disseminating corrections or amendments of PD to other authorized users of the PD.

Standard: ACME must implement mechanisms to correct, amend or append personal information based on information provided by the data subjects and communicates such information to third-parties, as committed or required, consistent with ACME's privacy commitments and system requirements. If a request for correction is denied, the data subject must be informed of the denial and reason for such denial consistent with ACME's privacy commitments and system requirements.

Guidelines: Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations apply discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought and the impact of the changes.

PRI-06(B): DATA SUBJECT ACCESS | NOTICE OF CORRECTION OR PROCESSING CHANGE

Control Objective: The organization notifies affected individuals if their Personal Data (PD) has been corrected or amended.

Standard: Where technically feasible and justified by a valid business case, data/process owners are required to notify affected individuals if their Personal Data (PD) has been corrected or amended.

Guidelines: Where Personal Data (PD) is corrected or amended, organizations take steps to ensure that all authorized recipients of such information and the individual with which the information is associated, are informed of the corrected or amended information.

PRI-06(C): DATA SUBJECT ACCESS | APPEAL ADVERSE DECISION

Control Objective: The organization provides an organization-defined process for individuals to appeal an adverse decision and have incorrect information amended.

Standard: Where technically feasible and justified by a valid business case, data/process owners are required to provides a process for individuals to appeal an adverse decision and have incorrect information amended.

Guidelines: The Senior Agency Official for Privacy ensures that practical means and mechanisms exist and are accessible for individuals to seek the correction or amendment of their Personal Data (PD). Redress processes are clearly defined and publicly available. Additionally, redress processes include the provision of responses to individuals of decisions to deny requests for correction or amendment. The responses include the reasons for the decisions, a means to record individual objections to the decisions and finally, a means of requesting reviews of the initial determinations.

PRI-06(D): DATA SUBJECT ACCESS | USER FEEDBACK MANAGEMENT

Control Objective: The organization implements a process for receiving and responding to complaints, concerns or questions from individuals about the organizational privacy practices that includes: [532]

- Mechanisms that are easy to use and readily accessible by the public;

[530] NIST 800-53 rev4 IP-2
[531] NIST 800-53 rev4 IP-3
[532] NIST 800-53 rev4 IP-4

Guidelines: None

PRM-03: Allocation of Resources

Control Objective: The organization:[542]

- Includes a determination of cybersecurity requirements for systems in business process planning;
- Determines, documents and allocates the resources required to protect systems as part of its capital planning and investment control process; and
- Establishes a discrete line item for cybersecurity in organizational programming and budgeting documentation.

Standard: The Chief Information Security Officer (CISO) 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. The CISO is required to:

(a) Include cybersecurity requirements in business process planning; and
(b) Allocate resources required to protect its systems and data, as part of its capital planning process.

Guidelines: To apply needed security controls within the Secure Development Life Cycle (SDLC) (including the acquisition process), it requires a basic understanding of cybersecurity, threats, vulnerabilities and risk to critical missions / business functions. Security engineering principles cannot be properly applied if individuals that design, code and test systems and system components (including information technology products that are used to build those systems / components) do not understand security. Therefore, ACME should include qualified cybersecurity personnel in SDLC activities to ensure that security requirements are incorporated into organizational systems.

PRM-04: Security & Privacy In Project Management

Control Objective: The organization: [543]

- Assesses the security controls in system project management 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) Data/process owners and asset custodians 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.

Guidelines: 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.

PRM-05: Security & Privacy Requirements Definition

Control Objective: The organization identifies security requirements for systems, system components and services at pre-defined decision points in the Secure Development Life Cycle (SDLC).[544]

Standard: Asset custodians, conjunction with data / process owners, are required to:

(a) Identify, define and document security requirements for systems, system components and services; and
(b) Update security requirements as business processes or other conditions change.

Guidelines: None

[542] NIST 800-53 rev4 SA-2 | NIST CSF v1.1 ID.BE-3
[543] NIST 800-53 rev4 CA-2 | ISO 27002:2013 6.1.5
[544] NIST 800-53 rev4 SA-14 | ISO 27002:2013 14.1 | NIST CSF v1.1 ID.BE-4 & ID.BE-5

Management Intent: The purpose of the Technology Development & Acquisition (TDA) policy is to ensure secure technologies are developed and / or acquired.

Policy: ACME shall implement the principles of "least privilege" and "least functionality in the development and implementation of technology, regardless if it is internally-developed or acquired from a third party. Technology development and acquisition must employ adequate security measures during all phases of the Secure Development Life Cycle (SDLC) to ensure security and privacy-related risks are identified and appropriately remediated.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide technology development and acquisition policy, as well as associated standards, controls and procedures.[598]

Standard: ACME's Procurement Department, in conjunction with the Chief Information Security Officer (CISO), is required to develop, implement and govern a formal acquisition program that:

(a) Incorporates cybersecurity and privacy principles; requirements; and
(b) Tailors acquisitions, contract tools and procurement methods to ensure compliance with applicable statutory, regulatory and contractual obligations.

Guidelines: None

TDA-01(A): TECHNOLOGY DEVELOPMENT & ACQUISITION | PRODUCT MANAGEMENT

Control Objective: The organization designs and implements products, applications and services to allow for security updates to correct security deficiencies.

Standard: ACME requires that products are designed and implemented to:

(a) Maintain appropriate documentation on how ACME provides validated software updates / patches throughout the product life cycle to assure its continued security;
(b) Allow for the application of security updates to the products software and firmware:
    1. Processes must support reverting to a previously-installed version if the update fails; and
    2. The roll-back would revert to the most recent installed version.
(c) Verify the authenticity and integrity of any software update through cryptographic means, prior to the installation of the update:
    1. Product updates must be possible in an offline environment; and
    2. Offline updates must also support the same authenticity and integrity validation process.
(d) Maintain at least one security-related event log that at a minimum contains the following events:
    1. Successful and unsuccessful login attempts;
    2. Change of user authentication credentials;
    3. Changes in the list of valid user accounts (e.g., addition, modification or deletion of accounts); and
    4. Successful and unsuccessful software updates.
(e) Prevent tampering of security-related event logs through transmitting logs to an external data storage location or security store the logs in non-volatile memory that prevents non-privileged users from deleting, moving or altering log file contents; and
(f) Enable secure decommissioning of the product by allowing users to securely purge or erase (e.g., zeroization) all user-defined data that includes:
    1. Configuration data; and
    2. Sensitive data.

Guidelines: None

[598] NIST 800-53 PL-1

TDA-01(B): TECHNOLOGY DEVELOPMENT & ACQUISITION | INTEGRITY MECHANISMS FOR SOFTWARE / FIRMWARE UPDATES

Control Objective: The organization employs integrity validation mechanisms for security updates.

Standard: ACME requires that products incorporate integrity mechanisms for software / firmware updates that include:

(a) Using a ACME code signing digital certificate to sign the software / firmware components; and
(b) Generating and publishing a Keyed-Hash Message Authentication Code (HMAC) value to provide assurance of the integrity of the following components:
    1. Binaries;
    2. Executables; and
    3. Libraries.

Guidelines: None

TDA-01(C): TECHNOLOGY DEVELOPMENT & ACQUISITION | MALWARE TESTING PRIOR TO RELEASE

Control Objective: The organization employs at least one (1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update.

Standard: ACME requires that products and updates incorporate malware testing by at least two (2) different malware detection tools in order to identify the existence of any known malware in the final deliverable:

(a) The malware tool must be applicable to for operating system that the software will be used on.
(b) All binary code and bytecode must be inspected for malware by automated tools.

Guidelines: None

TDA-02: SECURITY REQUIREMENTS

Control Objective: The organization includes the following requirements and / or specifications, explicitly or by reference, in system acquisitions based on an assessment of risk:[599]

- Security functional requirements / specifications;
- Security-related documentation requirements; and
- Developmental and evaluation-related security requirements.

Standard: Data/process owners and asset custodians are required to take security requirements into account when purchasing systems or outsourcing solutions.

Guidelines: None

TDA-02(A): SECURITY REQUIREMENTS | PORTS, PROTOCOLS & SERVICES IN USE

Control Objective: The organization requires the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.[600]

Standard: ACME requires that developers of systems, system components or services identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended that will be enabled for use in a production environment.

Guidelines: The identification of functions, ports, protocols and services early in the Secure Development Life Cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the system, system component or system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols or services (or when requiring system service providers to do so). Early identification of functions, ports, protocols and services avoids costly retrofitting of security controls after the system, system component or system service has been implemented.

[599] NIST 800-53 rev4 SA-4
[600] NIST 800-53 rev4 SA-4(9)

- SUPPLEMENTAL DOCUMENTATION -

DIGITAL SECURITY PROGRAM (DSP)

ANNEXES, TEMPLATES & REFERENCES

Version 2020.1

DSP
Digital Security Program

TABLE OF CONTENTS

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:

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 [Company Name].
		· Impact could include negatively affecting [Company Name]'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 [Company Name]
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'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 [Company Name], 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 [Company Name].
		· 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 [Company Name].
		· Impact would not be damaging or a risk to business operations.

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 [Company Name] 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 [Company Name] 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

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-[Company Name] employees.	▪ NDA is recommended prior to access by non-[Company Name] 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*

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.

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	

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 [Company Name], 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 [Company Name]:
  - 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 [Company Name]'s mission.
    - Cannot go down without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of [Company Name]'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 [Company Name]'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 [Company Name]'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		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

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 [Company Name].