YOUR LOGO GOES HERE

DIGITAL SECURITY PROGRAM (DSP)

ACME Business Consulting, Inc.

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, Inc. ([Company Name])'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 AI 100-1: *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
  - 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 800-63B, *Digital Identity Guidelines*
  - 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):
  - Center for Internet Security (**CIS**) Critical Security Controls (**CSC**)[3]
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[4]
  - Computer Security Incident Handling Guide[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]
  - Guide to Integrating Forensic Techniques into Incident Response[9]
  - Open Web Application Security Project (**OWASP**)[10]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[11]
  - Privacy by Design (**PbD**) [12]

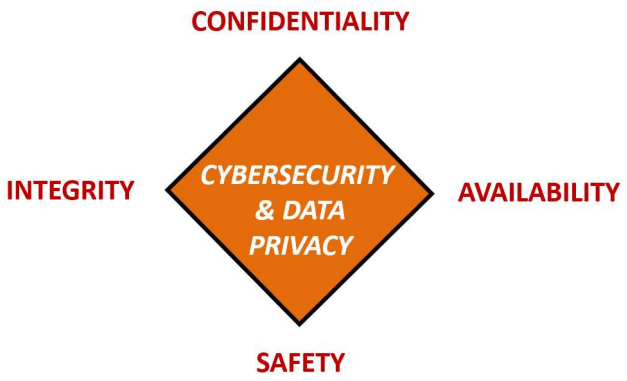
[1] National Institute of Standards and Technology - https://csrc.nist.gov/publications/sp
[2] International Organization for Standardization - https://www.iso.org/home.html
[3] Center for Internet Security - https://www.cisecurity.org/
[4] Cloud Security Alliance - https://cloudsecurityalliance.org/
[5] Computer Security Incident Handling Guide - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
[6] COBIT - https://www.isaca.org/resources/cobit
[7] DoD Information Security Agency - https://public.cyber.mil/
[8] DoD Cybersecurity Maturity Model Certification - https://www.acq.osd.mil/cmmc/index.html
[9] Guide to Integrating Forensic Techniques into Incident Response - https://csrc.nist.gov/publications/detail/sp/800-86/final
[10] OWASP - https://owasp.org/
[11] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/
[12] Term and principles coined by Dr. Ann Cavoukian - https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

INTRODUCTION

The **Digital Security Program (DSP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Business Consulting, Inc. ([Company Name]).

[Company Name] is committed to protecting its employees, partners, clients and [Company Name] from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with [Company Name] data and systems, applications and services. Therefore, it is the responsibility of both [Company Name] personnel and third-parties to be aware of and adhere to [Company Name]'s cybersecurity and data protection requirements.

Protecting [Company Name] data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, cybersecurity & data privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **CONFIDENTIALITY** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- **INTEGRITY** – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **AVAILABILITY** – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **SAFETY** – This addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

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 [Company Name] data and systems;
- Protecting [Company Name], its employees and its clients from illicit use of [Company Name] systems and data;
- Ensuring the effectiveness of security controls over data and systems that support [Company Name]'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 [Company Name]'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 [Company Name] 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 [Company Name] personnel understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help [Company Name] comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of [Company Name] data.

Scope & Applicability

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

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting [Company Name] business functions must comply with the standards. [Company Name] departments must 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.

[Company Name]'s documented roles and responsibilities provides a detailed description of [Company Name] user roles and responsibilities, in regard to cybersecurity-related use obligations.

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

Policy Overview

To ensure an acceptable level of cybersecurity risk, [Company Name] must 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.

[Company Name] personnel must 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 [Company Name] 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 [Company Name] systems and underlying data, occasionally exceptions will exist. When requesting an exception, users must 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 [Company Name] uses to define common cybersecurity terms.[13] 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 [Company Name] 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 [Company Name] 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 [Company Name] 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 data privacy stakeholder (or data 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 data 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 secure practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

Information Assurance: 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.

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.

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

MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION

The objective is to provide management direction and support for cybersecurity and data protection in accordance with business requirements and relevant laws and regulations. [17]

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind [Company Name]'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, [Company Name]'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, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Cybersecurity documentation is comprised of six (6) main parts:

(1) Policy that establishes management's intent;
(2) Control Objective that identifies leading practices (linked to controls);
(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.

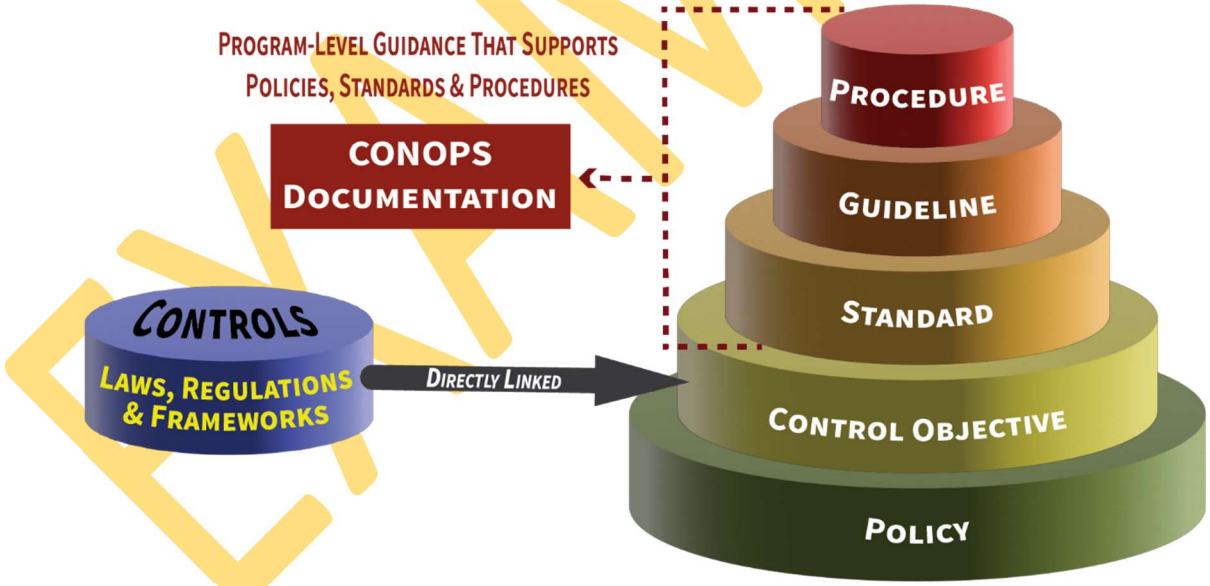


Figure 1. Cybersecurity Documentation Hierarchy

As referenced in this graphic, a Concept of Operations (CONOPS) is a cybersecurity-focused description that addresses life cycle concepts. This can include concepts for sustainment, logistics, maintenance and training. CONOPS augment and support an organization's policies, standards and procedures. Examples of CONOPS documentation includes, but is not limited to:

- Risk management (e.g., Risk Management Program (RMP))
- Vulnerability management (e.g., Vulnerability & Patch Management Program (VPMP))
- Incident response (e.g., Integrated Incident Response Program (IIRP))
- Business Continuity / Disaster Recovery (e.g., Continuity of Operations Plan (COOP))

[17] ISO 27002:2013 5.1

Management Intent: The purpose of the Cybersecurity & Data Protection (GOV) policy is to govern a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses all applicable statutory, regulatory and contractual obligations.

Policy: [Company Name] shall implement and maintain a maturity-based capability to strengthen the security and resilience of its technology infrastructure and data protection mechanisms against both physical and cyber threats. Security control decisions shall take applicable statutory, regulatory and contractual obligations into account, but [Company Name] acknowledges that being compliant does not equate to being secure, so all stakeholders shall protect the confidentiality, integrity, availability and safety of [Company Name]'s technology resources and data, regardless of the geographic location of the data or technology in use. Cybersecurity and data protection controls shall be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and technology in use.

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

GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

Control Objective: The organization facilitates the implementation of cybersecurity & data protection governance controls.[18]

Standard: [Company Name]'s cybersecurity & data protection policies and standards must be represented in a single document, the Digital Security Program (DSP) that:

(a) Must be reviewed and updated at least annually; and
(b) Disseminated to the appropriate parties to ensure all [Company Name] personnel understand their applicable requirements.

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

GOV-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STEERING COMMITTEE & PROGRAM OVERSIGHT

Control Objective: The organization coordinates cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.[19]

Standard: [Company Name] must establish a cybersecurity & data protection steering committee, or advisory board, comprised of key stakeholders from [Company Name] Lines of Business (LOB) and technology-related executives that:

(a) Meets formally and on a regular basis; and
(b) Receives briefings from the following:
    1. Chief Information Security Officer (CISO) on matters of cybersecurity;
    2. Chief Privacy Officer (CPO) on matters of data privacy ; and
    3. Chief Risk Officer (CRO) on matters of enterprise risk.

Guidelines: To achieve proper situational awareness across the organization, key cybersecurity & data privacy leaders must facilitate communication with business stakeholders. This includes translating cybersecurity, data privacy and risk concepts and language into business concepts and language as well as ensuring that business teams consult with cybersecurity & data privacy teams to determine appropriate controls measures when planning new business projects.

The steering committee, or advisory board, can best advise the CISO, CPO and CRO on important matters pertaining to the organization to ensure technology, cybersecurity & data privacy practices support the overall strategy and mission of the organization.

GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STATUS REPORTING TO GOVERNING BODY

Control Objective: The organization provides governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.

[18] ISO 27001-2013: 4.3, 4.4, 5.1, 6.1.1 | ISO 27002-2022: 5.1, 5.4, 5.37| NIST SP 800-53 R5: PM-1
[19] ISO 27001-2013: 4.3, 6.2, 7.4, 9.3, 10.2

Standard: [Company Name]'s Chief Information Security Officer (CISO) must:

(a) Operate a repeatable process for reporting to [Company Name]'s board of directors, or similar oversight function; and
(b) Provide detailed reporting, along with recommendations, to the oversight body; and
(c) Document feedback received.

Guidelines: None

GOV-02: Publishing Cybersecurity & Data Protection Documentation

Control Objective: The organization establishes, maintains and disseminates cybersecurity & data protection policies, standards and procedures. [20]

Standard: The Digital Security Program (DSP) document represents the consolidation of [Company Name]'s cybersecurity & data protection policies and standards.[21] The DSP is endorsed by [Company Name]'s executive management and shall be:

(a) Disseminated to the appropriate parties to ensure all affected personnel are made aware of and understand their applicable requirements to protect cardholder data;[22]
(b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the DSP, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;[23]
(c) Enforced by [Company Name] personnel through "business as usual" secure practices in the form of Standardized Operating Procedures (SOP) that shall be developed, enforced and maintained at the control operator level; and
(d) Enforced through [Company Name]'s supply chain in the form of contractual requirements with those third-parties that have the ability to directly or indirectly influence the confidentiality, integrity and/or availability of [Company Name]'s technology assets and/or sensitive/regulated data.

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

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. Without cybersecurity & data privacy policies, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its statutory, regulatory and/or contractual obligations, nor being able to adequately protect its technology and data in a consistent manner.

GOV-02.1: Publishing Cybersecurity & Data Protection Documentation | Exception Management

Control Objective: The organization prohibits exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.

Standard: For exception management purposes, [Company Name]:

(a) Prohibits any exception to a policy;
(b) Permits limited exceptions to a standard, when the following is met:
    1. Requests for exception to a standard are formally submitted to [Company Name]'s cybersecurity function;
    2. A legitimate business justification for deviation from the standard is provided;
    3. One (1), or more, compensating control(s) is/are implemented to reduce the risk associated with the deficient standard;
    4. A timeline for remediation is documented in a Plan of Action & Milestones (POA&M), or similar document, to track the deficiency through remediation.

Guidelines: For exception management purposes:

- A policy is defined as a high-level statement of management intent that exists to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by [Company Name]s executive leadership team.
- A standard is a mandatory requirement regarding processes, actions and configurations that is designed to satisfy a requirement (e.g., control, law, regulation, etc.).

[20] ISO 27001-2013: 4.3, 5.2, 7.5.1, 7.5.2, 7.5.3 | ISO 27002-2022: 5.1, 5.37| NIST SP 800-53 R5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1 | NIST CSF: ID.GV-1 | NIST SP 800-171A: 3.4.9[a], 3.9.2[a]
[21] NIST SP 800-171A R3 IPD: A.03.15.01.a[01]
[22] NIST SP 800-171A R3 IPD: A.03.15.01.a[02]
[23] NIST SP 800-171A R3 IPD: A.03.15.01.b[01], A.03.15.01.b[02]

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: [Company Name] shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. [Company Name] 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 facilitates the implementation of change management controls. [119]

Standard: [Company Name]'s Change Management Program requires data/process owners and asset custodians to test, validate and document changes to systems before implementing the changes on the production network. Changes for any production system, application and/or service must:

(a) Be:
    1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;[120]
    2. Approved by a [Company Name] employee with the appropriate authority and knowledge to understand the impact of the change;[121] and
    3. Approved by [Company Name]'s Change Control Board (CCB);
(b) Sufficiently document the following criteria to enable independent review:
    1. Reason for, and description of, the change;
    2. Documentation of security impact;
    3. Documented change approval by authorized parties;
    4. Functionality testing to verify the change:
        i. Did not adversely impact the security of the network; and
        ii. Performs as expected;
    5. For bespoke and custom software changes, all updates are tested for compliance with applicable statutory, regulatory and contractual obligations; and
    6. Procedures to address failures and return to a secure state;
(c) Ensure all applicable statutory, regulatory and contractual requirements are confirmed to be in place on all new or changed systems and networks; and
(d) As applicable, update affected documentation to include the changes to prevent inconsistencies between network documentation and the actual configuration.

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 data privacy or any combination thereof.

Due to the constantly changing state of pre- production environments, they are often less secure than the production environment. Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

Pre-production environments include development, testing, User Acceptance Testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre- production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

[119] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST CSF: PR.IP-3
[120] NIST SP 800-171A R3 IPD: A.03.04.03.b[01]
[121] NIST SP 800-171A R3 IPD: A.03.04.03.b[02]

CHG-02: Configuration Change Control

Control Objective: The organization governs the technical configuration change control processes.[122]

Standard: Data/process owners and asset custodians must follow [Company Name]'s 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 data) 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; and
    3. Functionality testing to verify that the change does not adversely impact the security of the system;
(f) Back-out procedures; and
(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 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-02.1: Configuration Change Control | Prohibition Of Changes

Control Objective: The organization prohibits unauthorized changes, unless organization-approved change requests are received.[123]

Standard: To prohibit unauthorized changes, [Company Name] requires:

(a) Data/process owners and asset custodians to:
    1. Prohibit implementing a change without first obtaining pre-approval from [Company Name]'s Change Control Board (CCB); and
    2. Notify all affected parties prior to the implementation of the change; and
(b) Where technically feasible, [Company Name] must utilize automated mechanisms to:
    1. Document proposed change(s);
    2. Notify affected stakeholders of proposed change(s);
    3. Request change approval;
    4. Highlight proposed changes that have not been approved or disapproved within an organization-defined time period;
    5. Prohibit change(s) until designated approval(s) is/are received;
    6. Document all changes; and
    7. Notify affected stakeholders when approved change(s) are completed.

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

CHG-02.2: Configuration Change Control | Test, Validate & Document Changes

Control Objective: The organization tests and documents proposed changes in a non-production environment before changes are implemented in a production environment.[124]

Standard: Data/process owners and asset custodians must:

(a) Where technically feasible, test and validate configuration changes in a test environment, prior to deploying the change in the production environment;[125] and

[122] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST CSF: PR.IP-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171A: 3.4.3[a], 3.4.3[b], 3.4.3[c], 3.4.3[d]
[123] NIST SP 800-53 R5: CM-3(1)
[124] ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3(2), CM-3(7), SA-8(31) | NIST SP 800-171 R2: NFO - CM-3(2)
[125] NIST SP 800-171A R3 IPD: A.03.04.03.c[02]

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 [Company Name]'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 statutory, regulatory and contractual obligations for cybersecurity and data protection, [Company Name] shall implement and maintain appropriate administrative, technical and physical security measures to protect the confidentiality, integrity and availability of its data, regardless if the data is in hardcopy or digital form. [Company Name] shall utilize methods of sanitizing or destroying digital and physical 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 facilitates the implementation of data protection controls. [344]

Standard: [Company Name]'s Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement:

(a) Controls to protect [Company Name] data wherever it is stored, transmitted and processed, in accordance with all applicable statutory, regulatory and contractual compliance obligations;
(b) Retention periods for both sensitive and non-sensitive/regulated data; and
(c) Processes to:
    1. Dispose of, destroy, erase and/or anonymizes data once it is no longer necessary for business purposes;
    2. Maintain strict control over the storage and accessibility of media; and
    3. Maintain inventories of sensitive/regulated data under [Company Name]'s 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-01.1: DATA PROTECTION | DATA STEWARDSHIP

Control Objective: The organization ensures data stewardship is assigned, documented and communicated. [345]

Standard: [Company Name]'s Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Data Protection Officer (DPO), or their designated representative(s), must:

(a) Develop and implement data stewardship practices that educate and train stakeholders how to:
    1. Physically secure all media with sensitive/regulated data;
    2. Maintain strict control over the storage and accessibility of media with sensitive/regulated data; and
    3. Maintain strict control over the internal or external distribution of any kind of media with sensitive/regulated data, including the following:
        i. Classify media so the sensitivity of the data can be determined; and
        ii. Send the media by secured courier or another delivery method that can be accurately tracked; and
(b) Require data/process owners and asset custodians to re-assess the following criteria, as it pertains to data stewardship on the systems, applications and services under their control:
    1. Data classification requirements;
    2. System criticality;
    3. Geographical storage and/or processing of the data; and
    4. Applicable statutory, regulatory and contractual requirements.

[344] ISO 27002-2022: 5.9, 5.10, 5.12, 5.33, 7.1, 8.12 | NIST SP 800-53 R5: MP-1 | NIST CSF: PR.DS-5 | NIST SP 800-171 R2: 3.8.1, NFO - MP-1 | NIST SP 800-171A: 3.8.1[a], 3.8.1[b], 3.8.1[c], 3.8.1[d]
[345] NIST SP 800-53 R5: SA-4(12)

Guidelines: See *Annex 4: Baseline Security Categorization Guidelines* for Safety & Criticality (SC) categorization. A complete inventory of mission-critical (SC1) and business-critical (SC2) 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-01.2: Data Protection | Sensitive/Regulated Data Protection

Control Objective: The organization protects sensitive/regulated data wherever it is stored.

Standard: Data/process owners and asset custodians must protect sensitive/regulated data from being stored in cleartext, where it is human-readable in storage media by:

(a) Configure systems, applications and services to render sensitive/regulated data unreadable anywhere it is stored by using any of the following approaches:
    1. One-way hashes based on strong cryptography of the sensitive/regulated data;
    2. Truncation;;
    3. Index tokens; and
    4. Strong cryptography;
(b) Review the following data sources to ensure that sensitive/regulated data is not retained in a human-readable format:
    1. Incoming transaction data;
    2. All logs (e.g., transaction, history, debugging, error);
    3. History files;
    4. Trace files;
    5. Database schemas;
    6. Contents of databases, and on-premises and cloud data stores; and
    7. Any existing memory/crash dump files;
(c) Rendering sensitive/regulated data unreadable anywhere it is stored; and
(d) Not tying user accounts to decryption keys.

Guidelines: The removal of cleartext sensitive/regulated data is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control.

Sources for information about index tokens include:

- PCI SSC's Tokenization Product Security Guidelines
- ANSI X9.119-2-2017: Retail Financial Services
- Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems

DCH-01.3: Data Protection | Sensitive / Regulated Media Records

Control Objective: The organization ensures media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.

Standard: Where technically feasible, [Company Name]'s Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement a metadata tracking and reporting capability for sensitive/regulated data that:

(a) Categorizes media records according to defined data classification categories;
(b) Identifies assets that contain sensitive/regulated data;
(c) Configures system event logging to provide appropriate situational awareness on activities associated with logical access to assets that contain sensitive/regulated data; and
(d) Provides the ability to determine the potential impact in the event of a data loss incident for identified sensitive/regulated data.

Guidelines: None

DCH-01.4: Data Protection | Defining Access Authorizations For Sensitive / Regulated Data

Control Objective: The organization explicitly defines authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.

Standard: Data/process owners must:

(a) Define specific roles for individuals and/or groups, as it pertains to business practices for interacting with sensitive/regulated data;

Management Intent: The purpose of the Technology Development & Acquisition (TDA) policy is to ensure technologies are developed and/or acquired according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.

Policy: [Company Name] shall implement and maintain secure development practices to strengthen the security and resilience of its developed technologies, regardless if the technology is internally-developed or acquired from a third-party provider. To reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses, technologies shall be developed according to a Secure Software Development Framework (SSDF) and tested throughout development to ensure secure development practices are implemented.

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

TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION

Control Objective: The organization facilitates the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.[1163]

Standard: [Company Name]'s Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement processes to govern a formal Technical Development & Acquisition (TDA) program that:

(a) Ensures acquisition strategies, contract tools and procurement methods:
    1. Identify supply chain risks;[1164]
    2. Protect against supply chain risks;[1165] and
    3. Mitigate supply chain risks;[1166]
(b) Incorporates cybersecurity & data privacy principles into the asset's lifecycle; and
(c) Tailors acquisitions, contract tools and procurement methods to ensure compliance with applicable statutory, regulatory and contractual obligations.

Guidelines: The acquisition process provides an important vehicle for protecting the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, the insertion of counterfeits, the insertion of malicious software or backdoors, and poor development practices throughout the system life cycle.

Organizations also consider providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security requirements of the organization. Contracts may specify documentation protection requirements.

TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION | PRODUCT MANAGEMENT

Control Objective: The organization designs and implements product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.[1167]

Standard: [Company Name] requires that products and/or services are proactively managed to:

(a) Maintain appropriate documentation on how [Company Name] 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

[1163] ISO 27002-2022: 8.25, 8.30 | NIST SP 800-53 R5: PL-1, SA-1, SA-4, SA-23 | NIST CSF: PR.DS-7 | NIST SP 800-171 R2: NFO - SA-4
[1164] NIST SP 800-171A R3 IPD: A.03.17.02[01]
[1165] NIST SP 800-171A R3 IPD: A.03.17.02[02]
[1166] NIST SP 800-171A R3 IPD: A.03.17.02[03]
[1167] NIST SP 800-53 R5: SA-23

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 an 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: It is often necessary for a system or system component that supports mission-essential services or functions to be enhanced to maximize the trustworthiness of the resource. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend on the organization-defined resources.

TDA-01.2: Technology Development & Acquisition | Integrity Mechanisms for Software/Firmware Updates

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

Standard: [Company Name] requires that products incorporate integrity mechanisms for software/firmware updates that include:

(a) Using a [Company Name] 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-01.3: Technology Development & Acquisition | Malware Testing Prior To Release

Control Objective: The organization utilizes 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: [Company Name] 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: Minimum Viable Product (MVP) Security Requirements

Control Objective: The organization ensures risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).[1168]

Standard: Data/process owners and asset custodians must:

(a) Take cybersecurity & data privacy requirements into account when purchasing systems or outsourcing solutions; and

[1168] ISO 27002-2022: 8.25, 8.29, 8.30 | NIST SP 800-53 R5: SA-4 | NIST SP 800-171 R2: NFO - SA-4

- SUPPLEMENTAL DOCUMENTATION -

DIGITAL SECURITY PROGRAM (DSP)

ANNEXES, TEMPLATES & REFERENCES

Version 2022.3

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 seven (7) sensitivity levels:

CUI-Restricted

Sensitive Personal Data (sPD)-Restricted

Personal Data (PD)-Restricted

Restricted

Confidential

Internal Use

Public

Classification		Data Sensitivity Description
Controlled Unclassified Information (CUI) - Restricted	**Definition**	CUI-Restricted information is U.S. Government regulated data that is highly-sensitive business information and the level of protection is dictated externally by both NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI-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 CUI-Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company's reputation.
Sensitive Personal Data (sPD) Restricted	**Definition**	Sensitive Personal Data (sPD) is a subset of Personal Data (PD) that is highly-sensitive information about individuals (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. sPD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the sPD is authorized to be stored, processed and/or transmitted.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if sPD Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements, damaging the company's reputation and posing a risk to identified individuals (e.g., identity theft, stalking, harassment, etc.).

Personal Data (PD) Restricted	**Definition**	Personal Data (PD) Restricted that is information that can identify an individual (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. The difference between sPD Restricted and PD Restricted is that PD Restricted information is publicly-available information (e.g., social media, news, court filings, etc.). PD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the PD Restricted is authorized to be stored, processed and/or transmitted, unless it is publicly-available information.
	Potential Impact of Loss	**· MODERATE DAMAGE would occur if PD Restricted information were to become available to unauthorized parties either internal or external to ACME.** **· Impact could include negatively affecting ACME's competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company's reputation.**
Restricted	**Definition**	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is generally dictated externally by statutory, regulatory and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements and posing an identity theft risk.
Confidential	**Definition**	Confidential information is highly-valuable, sensitive business information and the level of protection is dictated internally by ACME.
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME's competitive position, damaging the company's reputation and violating contractual requirements.
Internal Use	**Definition**	Internal Use information is information originated or owned by ACME or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME. · Impact could include damaging the company's reputation and violating contractual requirements.
Public	**Definition**	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· NO DAMAGE would occur if Public information were to become available to parties either internal or external to ACME. · Impact would not be damaging or a risk to business operations.

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**. CUI-Restricted, 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
  - Other biometric data:
    - Retina scan;
    - Voice signature; and
    - Facial geometry; and
- Linkable Information
  - Date of birth;

DATA HANDLING GUIDELINES

Note: For U.S. Government regulated data, the following requirements supersede ACME data handling guidelines:

- *For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handing:*
  - *48 CFR § 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))*
- *For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handing:*
  - *32 CFR § 2002*
  - *DoD Instruction 5200.48*
  - *NIST SP 800-171 rev2*

Handling Controls	CUI - RESTRICTED	Restricted	Confidential	Internal Use	Public
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non- employees.	▪ NDA is required prior to access by non- employees.	▪ NDA is recommended prior to access by non-employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-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*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended	*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 groups	▪ Encryption is required ▪ 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	▪ 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

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	PD - Restricted	sPD - Restricted	CUI - Restricted
Non-Public Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	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	
	Geolocation Information (e.g., precise geographic location and/or history)						X	
	Race / Ethnicity						X	
	Religious Affiliation						X	
	Union Membership						X	
	Philosophical Beliefs						X	
	Private Communications (e.g., contents of private mail, emails and text messages)						X	
	Genetic Information						X	
	Biometrics						X	
	Health Information						X	
	Sexual Orientation						X	
	Birth Date						X	
	First & Last Name						X	
	Age						X	
	Phone Number						X	
	Home Address						X	
	Gender						X	
	Email Address						X	
Publicly Available Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Geolocation Information (e.g., precise geographic location and/or history)					X		
	Race / Ethnicity					X		
	Religious Affiliation					X		
	Union Membership					X		
	Philosophical Beliefs					X		
	Private Communications (e.g., contents of private mail, emails and text messages)					X		
	Health Information					X		
	Sexual Orientation					X		
	Birth Date					X		
	First & Last Name					X		
	Age					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).*

SAFETY & CRITICALITY

One component of assessing risk is to understand the criticality of systems and data. By having a clear understanding of the Safety & Criticality Level (SC) for an asset, system, application, service or data, determining potential impact will be more accurate.

There are four (4) SC levels:

1. Mission Critical (SC1);
2. Business Critical (SC2);
3. Non-Critical (SC3); and
4. Business Supporting (SC4).

MISSION CRITICAL (SC1)

Mission Critical (SC1) assets handle information that is determined to be vital to the operations or mission effectiveness of ACME.

The impact of a SC1 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide business stoppage with significant revenue impact can be anything that creates a significant impact on ACME's ability to perform its mission;
- Public, wide-spread damage to ACME's reputation;
- Direct, negative & long-term impact on customer satisfaction; and
- Risk to human health or the environment.

Examples of SC1 systems, applications and services include, but are not limited to:

- *Enterprise Resource Management (ERM) system (e.g., SAP)*
- *Active Directory (AD)*
- *Ability to process Point of Sale (PoS) or eCommerce payments*

BUSINESS CRITICAL (SC2)

Business Critical (SC2) assets handle information that is important to the support of ACME's primary operations.

The impact of a SC2 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide delay or degradation in providing important support services that may seriously impact mission effectiveness or the ability to operate;
- Department-level business stoppage with direct or indirect revenue impact; and
- Direct, negative & short-term impact on customer satisfaction.

Examples of SC2 systems, applications and services include, but are not limited to:

- *Email (e.g., Exchange)*
- *Payroll systems*
- *Corporate website functionality*
- *Corporate mobile device application functionality*
- *HVAC systems*
- *Customer support / call center functionality*

NON-CRITICAL (SC3)

Non-Critical (SC3) assets handle information that is necessary for the conduct of day-to-day business, but they are not mission critical in the short-term.

The impact of a SC3 system, or its data, being unavailable includes, but is not limited to:

- Widespread delays or degradation of services or routine activities;
- Widespread employee productivity degradation;