YOUR LOGO GOES HERE

SECURITY, COMPLIANCE & RESILIENCE PROGRAM (SCRP)

ACME Business Consulting, Inc.

SENSITIVE

Access Limited to Authorized Personnel

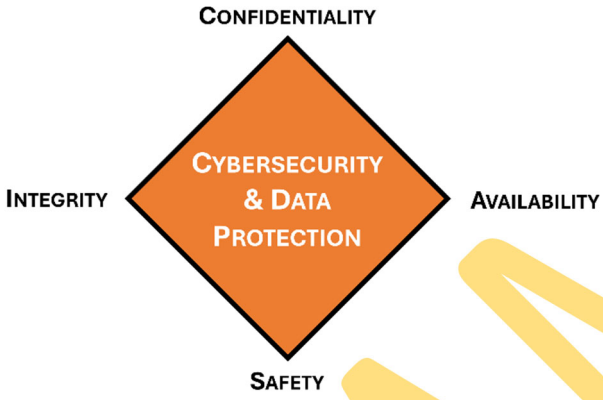
Table of Contents

MANAGEMENT COMMITMENT

The **Security, Compliance & Resilience Program (SCRP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Business Consulting, Inc. (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with ACME's Technology Assets, Applications, Services and/or Data (TAASD). Therefore, it is the responsibility of both ACME personnel and third-parties to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, cybersecurity and data protection measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of TAASD. This also includes protection against accidental loss or destruction. The protection of TAASD must include 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 Security, Compliance & Resilience Program (SCRP) is to:

- Create a leading practice-based Security, Compliance & Resilience Management System (SCRMS);
- Protect the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME data and systems;
- Protect ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensure the effectiveness of cybersecurity and data protection controls over data and systems that support ACME's operations; and
- Provide for the development, review and maintenance of the cybersecurity and data protection 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 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 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.

People, Processes, Technology, Data & Facilities (PPTDF) Control Applicability

Control scoping does not mean all controls apply uniformly to every asset, individual or facility. This misunderstanding of applicability vs scoping is one of the biggest hurdles that organizations face, since there is a common misconception that if something is "in scope" then every control will be applicable across the entire boundary of the assessment. This is an incorrect assumption. When looking at the breath of controls that an organization is obligated to comply with, the controls are often administrative, technical or physical in nature. This means that there may be controls that are not applicable to certain systems, applications and/or processes.

Example 1: Network firewall

- A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- A network firewall is a device. Therefore, a network firewall is not capable of undergoing end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.

Example 2: User awareness training

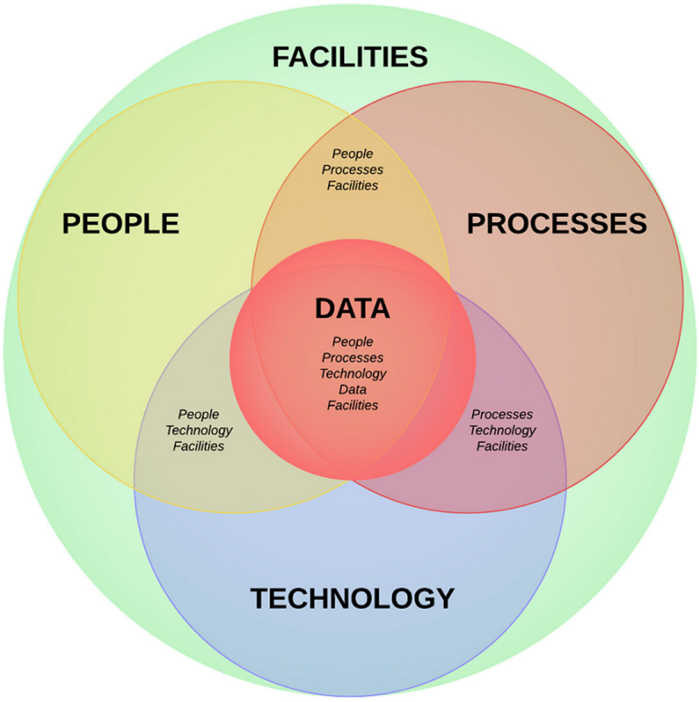
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.

Example 3: Incident Response Plan (IRP)

- An IRP is a documented process that guides incident response operations.
- An IRP is not an individual or technology. Therefore, an IRP cannot sign an NDA, have MFA or be patched.

The People, Processes, Technology, Data and Facilities (PPTDF) model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls.

- People. Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
- Processes. Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
- Technology. Control directly applies to Technology Assets, Applications and/or Services (TAAS) (e.g., secure baseline configurations, patching, etc.).
- Data. Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
- Facilities. Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



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

ACME's documented roles and responsibilities provides a detailed description of ACME user roles and responsibilities, in regard 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 must be effective immediately upon approval by management unless otherwise stated.

Roles

As part of ACME's Human Resources (HR) department's function to facilitate the implementation of personnel security controls, HR is required to assign all employees and contractors with one, or more, defined roles. Those roles are designed to manage personnel security risk by:

- Assigning a risk designation to all position; and
- Establishing screening criteria for individuals filling those positions

Responsibilities

To ensure an acceptable level of cybersecurity risk, ACME must design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems. The SCRP 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 the SCRP's policies, standards and guidelines.

ACME 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 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 must submit a business justification for deviation from the standard in question.

Updates To Policies & Standards

Updates to the Security, Compliance & Resilience Program (SCRP) 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.

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 and data protection principles that addresses all applicable statutory, regulatory and contractual obligations.

Policy: ACME shall tailor cybersecurity and data protection controls accordingly so that cost-effective controls can be applied commensurately with the risk and sensitivity of the data and technologies in use, ensuring applicable security, compliance and resilience requirements are sufficiently addressed.

ACME 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 ACME acknowledges that being compliant does not equate to being secure, so all stakeholders shall protect the confidentiality, integrity, availability and safety of ACME's technology resources and data, regardless of the geographic location of the data or 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 and data protection governance controls.[22]

Standard: ACME's cybersecurity and data protection policies and standards must be represented in a single document, the Security, Compliance & Resilience Program (SCRP) that:

(a) Must 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 SCRP together provide complete coverage for all cybersecurity and data protection-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.[23]

Standard: ACME must establish a cybersecurity and data protection steering committee, or advisory board, comprised of key stakeholders from ACME 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 and data protection 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 and data protection teams to determine appropriate controls measures when planning new business projects.

[22] *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 | NIST SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV, GV.RM-01, GV.RM-03, GV.RR-01, GV.SC, GV.SC-01, GV.SC-03, GV.SC-09, ID.RA, PR, PR.IR*
[23] *ISO 27001-2013: 4.3, 6.2, 7.4, 9.3, 10.2 | NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.OV, GV.OV-01, GV.OV-02, GV.OV-03, GV.RM-01, GV.RM-03, GV.RR-01, GV.SC, GV.SC-01, GV.SC-03, GV.SC-09, ID, ID.RA, PR, PR.IR*

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 and data protection 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 its cybersecurity and data protection program.[24]

Standard: ACME's Chief Information Security Officer (CISO) must:

(a) Operate a repeatable process for reporting to ACME'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-01.3: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | COMMITMENT TO CONTINUAL IMPROVEMENTS

Control Objective: The organization commits appropriate resources needed for continual improvement of the organization's cybersecurity and data protection program, including:

(1) Staffing;
(2) Budget;
(3) Processes; and
(4) Technologies.

Standard: ACME must:

(a) Appropriate necessary resources needed for continual improvement of the organization's cybersecurity and data protection program, including:
    1. Staffing;
    2. Budget;
    3. Processes; and
    4. Technologies.
(b) Operate a repeatable process for reporting to ACME's board of directors, or similar oversight function, that:
    1. Provides detailed reporting, along with recommendations, to the oversight body; and
    2. Documents feedback received.

Guidelines: None

GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

Control Objective: The organization establishes, maintains and disseminates cybersecurity and data protection policies, standards and procedures. [25]

Standard: The Security, Compliance & Resilience Program (SCRP) document represents the consolidation of ACME's cybersecurity and data protection policies and standards. The SCRP is endorsed by ACME'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;
(b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the SCRP, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;
(c) Enforced by ACME 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

---

[24] *NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.OV, GV.OV-01, GV.OV-03, GV.SC, GV.SC-09, ID*
[25] *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 SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV.PO, GV.PO-01, GV.SC-01, GV.SC-03, ID.RA*

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change in a unified effort to prevent business disruptions and unintended outcomes. Without properly documented and implemented change controls, cybersecurity and data protection 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 that affect Technology Assets, Applications, Services and/or Data (TAASD).

Policy: ACME shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change affecting production Technology Assets, Applications, Services and/or Data (TAASD).

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. [140]

Standard: ACME'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 Technology Assets, Applications and/or Services (TAAS) must:

(a) Be:
    1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;
    2. Approved by a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
    3. Approved by ACME's Change Control Board (CCB);
(b) Sufficiently document the following criteria to enable independent review:
    1. Reason for, and description of, the change;
    2. Security impact;
    3. 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.

---

[140] *ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a | CSF 2.0: ID.RA-07*

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.

CHG-02: Configuration Change Control

Control Objective: The organization governs the technical configuration change control processes.[141]

Standard: Data/process owners and asset custodians must follow ACME'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.[142]

Standard: To prohibit unauthorized changes, ACME requires:

(a) Data/process owners and asset custodians to:
    1. Prohibit implementing a change without first obtaining pre-approval from ACME's Change Control Board (CCB); and
    2. Notify all affected parties prior to the implementation of the change; and
(b) Where technically feasible, ACME 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.

---

[141] *ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a, 03.04.03.b, 03.04.03.c | NIST CSF 2.0: ID.RA-07*

[142] *NIST SP 800-53 R5: CM-3(1) | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a | NIST CSF 2.0: ID.RA-07*

Management Intent: The purpose of the Data Classification & Handling (DCH) policy is to ensure that Technology Assets, Applications, Services and/or Data (TAASD) 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 sensitive/regulated data.

Policy: In accordance with all applicable statutory, regulatory and contractual obligations for cybersecurity and data protection, ACME shall implement and maintain appropriate administrative, technical and physical security measures for its Technology Assets, Applications and/or Services (TAAS) to protect the confidentiality, integrity and availability of its data, regardless if the data is in hardcopy or digital form. ACME 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. [288]

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

(a) Controls to protect ACME 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 ACME'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.[289]

Standard: ACME'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 Technology Assets, Applications and/or Services (TAAS) under their control:
    1. Data classification requirements;
    2. System criticality;
    3. Geographical storage and/or processing of the data; and

[288] *ISO 27002-2022: 5.9, 5.10, 5.12, 5.33, 7.1, 8.12 | NIST SP 800-53 R5: MP-1 | NIST SP 800-171 R2: 3.8.1, 3.8.3, NFO - MP-1 | NIST SP 800-171 R3: 03.01.01.d.01, 03.01.01.d.02, 03.08.01 | NIST CSF 2.0: ID.AM-08, PR.DS, PR.DS-01, PR.DS-02, PR.DS-10 | FAR 52.204-21(b)(1)(vii)*
[289] *NIST SP 800-53 R5: SA-4(12) | NIST SP 800-171 R3: 03.08.01, 03.08.05.a | NIST CSF 2.0: ID.AM-08, PR.DS*

4. Applicable statutory, regulatory and contractual requirements.

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 processed and/or stored.[290]

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) Configuring Technology Assets, Applications and/or Services (TAAS) to render sensitive/regulated data unreadable anywhere it is processed and/or 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) Reviewing 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. [291]

Standard: Where technically feasible, ACME'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.

---

[290] *NIST SP 800-171 R2: 3.10.6 | NIST SP 800-171 R3: 03.01.01.d.01, 03.01.01.d.02, 03.01.02, 03.01.20.a, 03.01.20.b, 03.01.20.c.01, 03.01.20.d, 03.06.05.d, 03.08.01, 03.08.02, 03.08.05.a, 03.17.01.c | NIST CSF 2.0: PR.DS | FAR 52.204-21(b)(1)*
[291] *NIST SP 800-171 R3: 03.08.05.c | NIST CSF 2.0: PR.DS*

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 that could affect ACME's Technology Assets, Applications, Services and/or Data (TAASD).

Policy: ACME shall implement and maintain secure development practices to strengthen the security and resilience of its developed technologies, regardless if the Technology Asset, Application and/or Service (TAAS) is internally-developed or acquired from a third-party provider. To reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses, TAAS 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.[873]

Standard: ACME'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;
    2. Protect against supply chain risks; and
    3. Mitigate supply chain risks;
(b) Incorporates cybersecurity and data protection 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 proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:[874]

(1) Improve functionality;
(2) Enhance security and resiliency capabilities;
(3) Correct security deficiencies; and

[873] *ISO 27002-2022: 8.25, 8.30 | NIST SP 800-53 R5: PL-1, SA-1, SA-4, SA-23 | NIST SP 800-171 R2: NFO - SA-4 | NIST SP 800-171 R3: 03.12.01, 03.12.03, 03.14.01.a, 03.16.01, 03.17.02 | NIST CSF 2.0: ID.RA-09, PR.PS-06*
[874] *NIST SP 800-53 R5: SA-23 | NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.SC-09, PR.PS-06*

(4) Conform with applicable statutory, regulatory and/or contractual obligations.

Standard: ACME's Technology Assets, Applications and/or Services (TAAS) must be proactively managed to:

(a) Govern the design, development and production of TAAS across the System Development Life Cycle (SDLC) to:
    1. Improve functionality;
    2. Enhance security and resiliency capabilities;
    3. Correct security deficiencies; and
    4. Conform with applicable statutory, regulatory and/or contractual obligations; and
(b) Maintain appropriate documentation on how ACME provides validated software updates/patches throughout the product life cycle to assure its continued security;
(c) Allow for the application of security updates to the product's 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.
(d) 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.
(e) Build security features into TAAS, including:
    1. Maintaining situational awareness through an event log that, at a minimum, contains the following events:
        i. Successful and unsuccessful login attempts;
        ii. Change of user authentication credentials;
        iii. Changes in the list of valid user accounts (e.g., addition, modification or deletion of accounts); and
        iv. Successful and unsuccessful software updates; and
    2. 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.[875]

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-01.3: 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.

---

[875] *NIST CSF 2.0: ID.RA-09*

- SUPPLEMENTAL DOCUMENTATION -

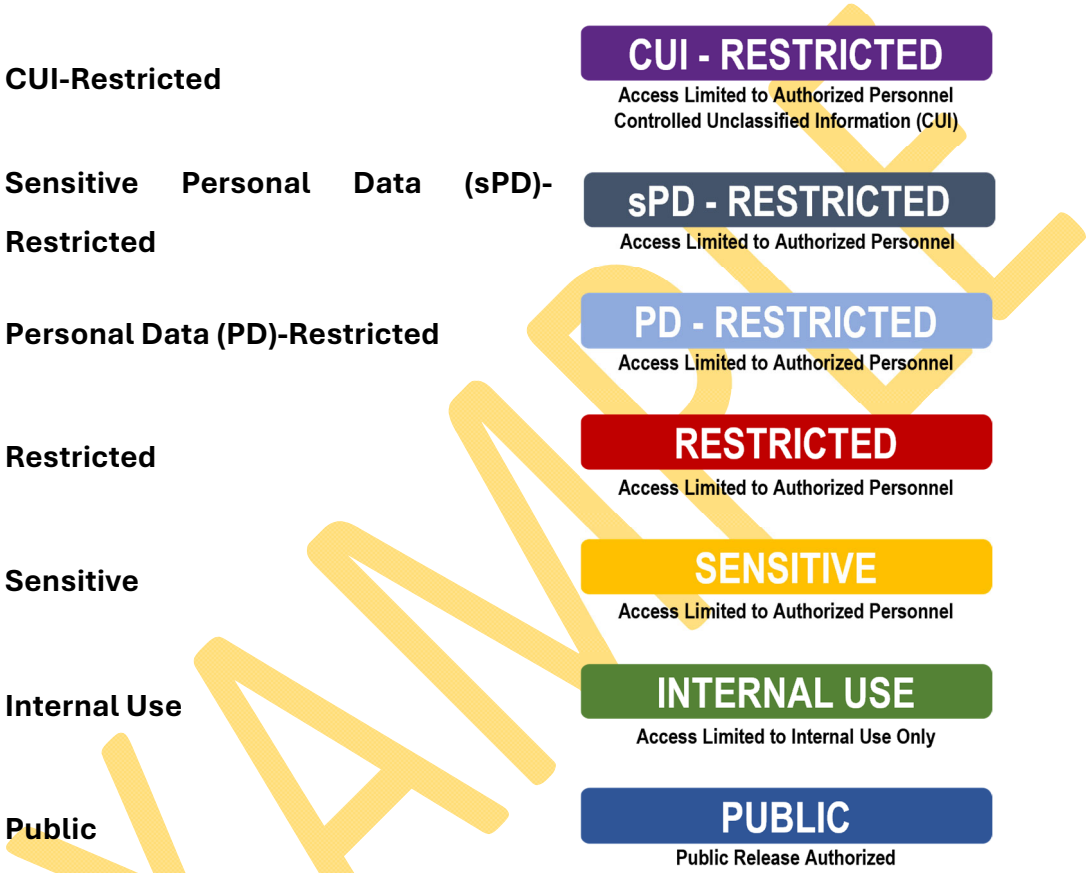
SECURITY, COMPLIANCE & RESILIENCE PROGRAM
ANNEXES, TEMPLATES & REFERENCES

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:



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.
Sensitive	**Definition**	Sensitive 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 Sensitive 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.

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 Part 170*
  - *DoD Instruction 5200.48*
  - *NIST SP 800-171*

Handling Controls	CUI - RESTRICTED	Restricted	Sensitive	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	Sensitive	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		

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;