YOUR LOGO GOES HERE

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

NIST Cybersecurity Framework 2.0

ACME Consulting Partners, LLP

SENSITIVE

Access Limited to Authorized Personnel

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 Consulting Partners, LLP (ACME)'s Technology Assets, Applications and/or Services (TAAS) 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 Cybersecurity And Data Protection Program (CDPP):

- The National Institute of Standards and Technology (NIST): [1]
  - NIST AI 100-1: *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
  - NIST AI 600-1: *Trustworthy and Responsible AI*
  - 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]

---

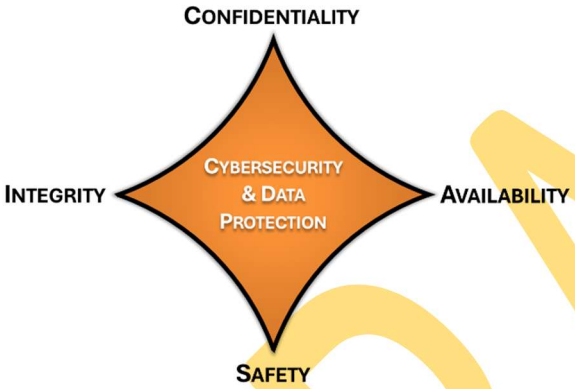
[1] *National Institute of Standards and Technology* - https://csrc.nist.gov/publications/sp
[2] *International Organization for Standardization* - https://www.iso.org/home.html
[3] *Center for Internet Security* - https://www.cisecurity.org/
[4] *Cloud Security Alliance* - https://cloudsecurityalliance.org/
[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

MANAGEMENT COMMITMENT

The **Cybersecurity And Data Protection Program (CDPP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Consulting Partners, LLP (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 Cybersecurity And Data Protection Program (CDPP) is to:

- Create a leading practice-based Information Security Management System (ISMS);
- 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

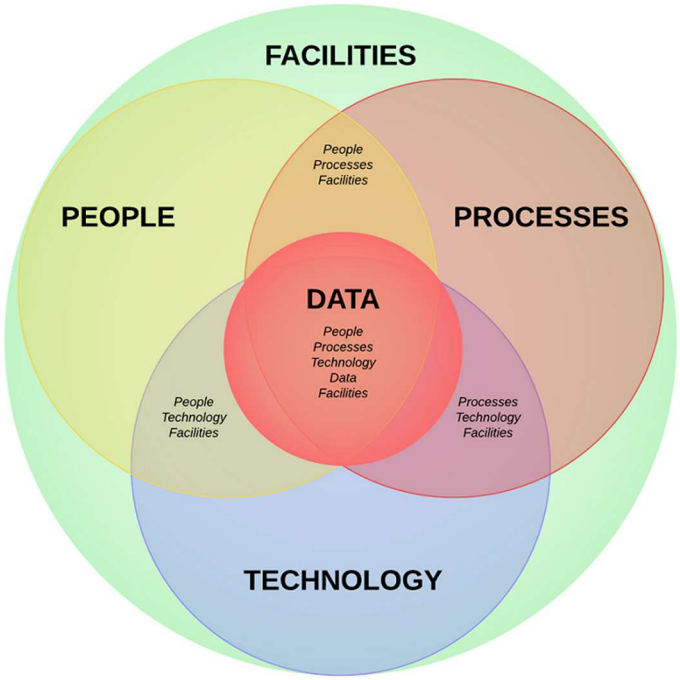
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual 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 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 CDPP 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 CDPP'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.

Key Terminology

ACME recognizes two (2) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[13] and

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

- NIST Glossary.[14]

From the context of this document, it is important to clarify mandatory versus optional criteria:[15]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

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.

Artificial Intelligence and Autonomous Technologies (AI/ML): A term describing tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.

Assessment Objective (AO): A term describing objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.

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

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

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

Compensating Control: A term describing an alternative cybersecurity and/or data protection controls implemented in lieu of the intended control(s) that provide equivalent, or comparable protection.

Conflict of Interest (COI): A term describing situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.

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

Control Inheritance: A term describing a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

---

[14] *NIST Glossary - https://csrc.nist.gov/glossary*
[15] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*

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 Cybersecurity And Data Protection Program (CDPP) 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 CDPP 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-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 Cybersecurity And Data Protection Program (CDPP) document represents the consolidation of ACME 's cybersecurity and data protection policies and standards. The CDPP 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 CDPP, 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
(d) Enforced through ACME '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 ACME 's Technology Assets, Applications and/or Services (TAAS) and/or sensitive/regulated data.

Guidelines: An organization's cybersecurity policies create the roadmap for implementing cybersecurity and data protection 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 and data protection 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.[26]

Standard: For exception management purposes, ACME :
(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 ACME 's cybersecurity function;
    2. A legitimate business justification for deviation from the standard is provided;

---

[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*
[26] *NIST CSF 2.0: ID.RA-07*

Management Intent: The purpose of the Compliance (CPL) policy is to govern the execution of cybersecurity and data protection controls to create appropriate evidence of due diligence and due care, demonstrating reasonable compliance with all applicable statutory, regulatory and contractual obligations.

Policy: ACME shall ensure appropriate technical, administrative and/or physical controls exist to provide sufficient evidence of due diligence and due care that reasonably demonstrate compliance with all applicable statutory, regulatory and contractual obligations. These security controls shall be reasonably-designed, properly-implemented and proactively-managed to protect sensitive/regulated business data and Technology Assets, Applications and/or Services (TAAS) against loss, unauthorized access and/or disclosure.

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

CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE

Control Objective: The organization facilitates the identification and implementation of relevant statutory, regulatory and contractual controls.[75]

Standard: Data/process owners and asset custodians must protect ACME 's systems and data in accordance with applicable statutory, regulatory and contractual compliance obligations.

Guidelines: See *Annex 4: Baseline Security Categorization Guidelines* for Safety & Criticality (SC) categorization. The requirements for defining critical infrastructure and key resources are found in applicable laws, regulations and contract requirements.

CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE | COMPLIANCE SCOPE

Control Objective: The organization documents and validates the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.[76]

Standard: ACME 's Chief Information Security Officer (CISO), or the CISO's designated representative(s) perform either a continuous or annual, documented review of cybersecurity and data protection scoping that utilizes comprehensive analysis and appropriate technical measures as follows:

(a) Verification must be performed upon significate change to:
    1. The in-scope environment (e.g., statutory, regulatory and/or contractual); and
    2. Organizational structure that could potentially impact compliance efforts;
(b) At a minimum, the scoping validation must include:
    1. Identifying all data flows for the sensitive/regulated data;
    2. Identifying all locations where sensitive/regulated data is stored, processed, and transmitted, including but not limited to:
        A. Any locations outside of the currently defined Sensitive Data Enclave (SDE);
        B. Applications that process sensitive/regulated data;
        C. Transmissions between systems and networks; and
        D. File backups;
    3. Identifying all system components in the SDE, connected to the SDE, or that could impact security of the SDE;
    4. Identifying all segmentation controls in use and the environment(s) from which the SDE is segmented, including justification for environments being out of scope;
    5. Identifying all connections from third-party entities with access to the SDE; and
    6. Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the SDE are included in scope; and

[75] *ISO 27002-2022: 5.31, 8.34 | NIST SP 800-53 R5: PL-1, PM-8 | NIST SP 800-171 R2: NFO - PL-1 | NIST SP 800-171 R3: 03.04.11.a, 03.12.01 | FAR 52.204-21(b)(2), 52.204-21(c) | NIST CSF 2.0: GV.OC, GV.OC-03, GV.SC-05, PR*

[76] *NIST SP 800-171 R3: 03.04.11.a, 03.15.02.a.04 | NIST CSF 2.0: GV.SC-05*

(c) Results are communicated to ACME 's executive management.

Guidelines: This annual confirmation of compliance scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.

Accurate scoping involves critically evaluating the SDE and all connected system components to determine the necessary coverage. Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured. When documenting account data locations, the entity can consider creating a table or spreadsheet that includes the following information:

- Data stores (databases, files, cloud, etc.), including the purpose of data storage and the retention period;
- How data is secured (type of encryption and strength, hashing algorithm and strength, truncation, tokenization); and
- How access to data stores is logged, including a description of logging mechanism (s) in use (enterprise solution, application level, operating system level, etc.).

A data discovery tool or methodology can be used to facilitate identifying all sources and locations of sensitive/regulated data. This approach can help ensure that previously unknown locations of sensitive/regulated data are detected and that it is either eliminated or properly secured.

CPL-02: Cybersecurity & Data Protection Controls Oversight

Control Objective: The organization provides a cybersecurity and data protection controls oversight function that reports to its executive leadership.[77]

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

(a) Utilize a robust cybersecurity and data protections controls framework that captures statutory, regulatory and contractual requirements relevant to ACME 's needs; and

(b) Establish and maintain a process to:
   1. Continuously improve both detection and protection processes;
   2. Employ assessors or assessment teams with reasonable independence to monitor cybersecurity and data protection controls in the system on an ongoing basis;
   3. Review the control framework at least annually to ensure changes that could affect the business processes are reflected;
   4. Maintain documentation of the review process to include:
      i. Documenting results of the reviews; and
      ii. Review and sign-off of results by authorized personnel; and
   5. Present results of cybersecurity and data protection controls oversight to the organization's risk and/or audit committee(s); and

(c) At least every twelve (12) months, or when there are significant incidents, or significant changes to risks, perform reviews of security operations to ensure that ACME adequately addresses nonconformities of established policies, standards, procedures and compliance obligations. At a minimum, the reviews must cover the following processes:
   1. Daily log reviews;
   2. Firewall ruleset reviews;
   3. Applying configuration standards to new systems;
   4. Responding to security alerts;
   5. Access management practices; and
   6. Change management processes.

Guidelines: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not:

- Create a mutual or conflicting interest with the organizations where the assessments are being conducted;

---

[77] *ISO 27001-2013: 9.1, 9.3, 10.2 | ISO 27002-2022: 5.31, 5.36, 6.8, 8.8, 8.34 | NIST SP 800-53 R5: CA-7, CA-7(1), PM-14 | NIST SP 800-171 R2: 3.12.1, 3.12.3 | NIST SP 800-171 R3: 03.12.01, 03.12.03 | NIST CSF 2.0: GV.OC-03*

- SUPPLEMENTAL DOCUMENTATION -

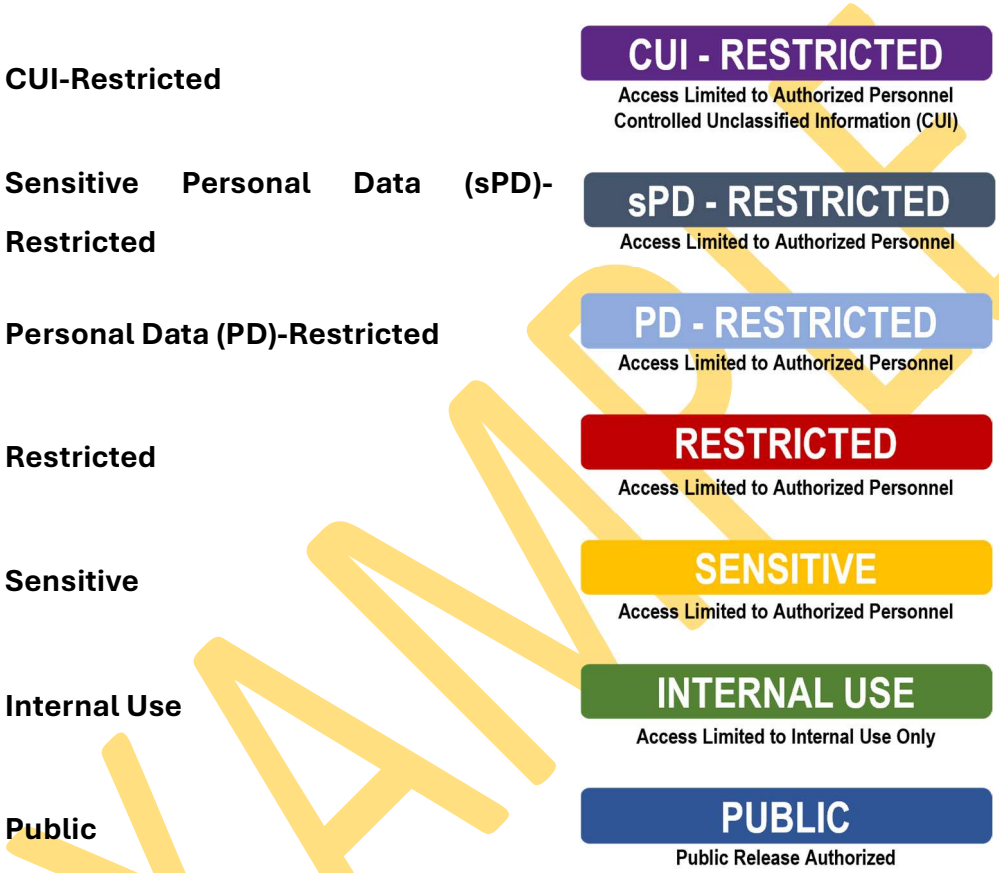
ANNEXES, TEMPLATES & REFERENCES

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.

	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 Sensitive 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 Sensitive information, the entire application is Sensitive.
- Restricted, Sensitive 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 in the United States (US) include, but are not limited to: [1]

- An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social security number.
  - Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
  - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  - Medical information.
  - Health insurance information.
  - Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

[1] *CA Civil Code 1798.81.5 - https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5*

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 3: DATA RETENTION SCHEDULE

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

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

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

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;