CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

CMMC Level 1 / FAR 52.204-21

ACME Professional Services, LLP

SENSITIVE
Access Limited to Authorized Personnel

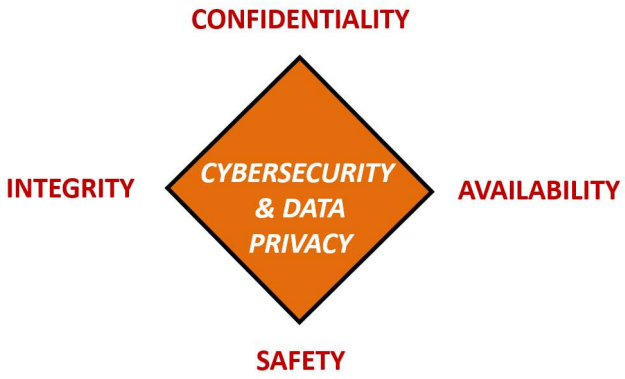
Table of Contents

MANAGEMENT COMMITMENT

The **Cybersecurity & Data Protection Program (CDPP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Professional Services, 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 security of Technology Assets, Applications and/or Services (TAAS) must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



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

PURPOSE

The purpose of the Cybersecurity & 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

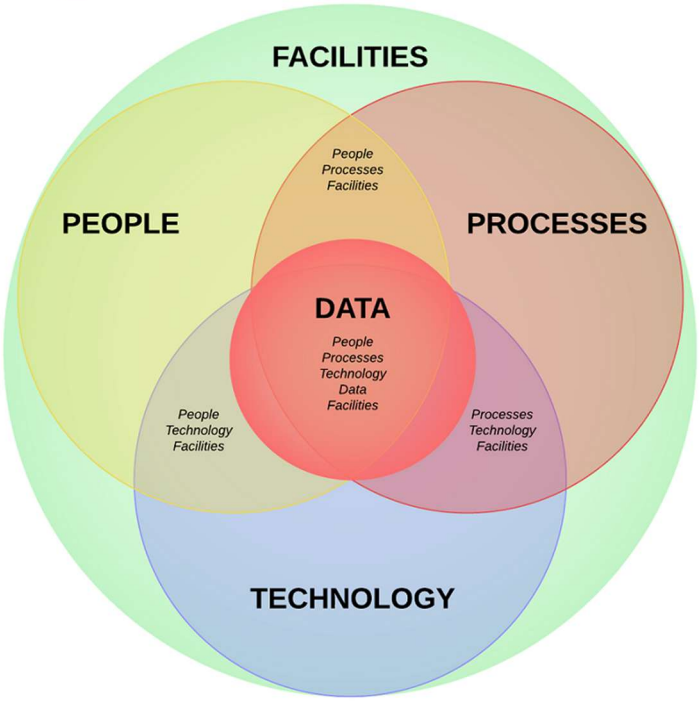
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual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



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.[10]

Standard: ACME's cybersecurity and data protection policies and standards must be represented in a single document, the Cybersecurity & 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 DSP together provide complete coverage for all cybersecurity and data protection-related controls employed within the organization.

GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

Control Objective: The organization establishes, maintains and disseminates cybersecurity and data protection policies, standards and procedures.[11]

Standard: The Cybersecurity & Data Protection Program (CDPP) document represents the consolidation of ACME's cybersecurity and data protection policies and standards. The DSP 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 DSP, 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.

---

[10] *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*

[11] *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 Asset Management (AST) policy is to ensure that Technology Assets, Applications and/or Services (TAAS) are properly managed throughout the lifecycle of the asset, from procurement through disposal.

Policy: ACME shall implement and maintain appropriate IT Asset Management (ITAM) practices to strengthen the security, compliance and resilience of its technology infrastructure and data protection capabilities against both physical and cyber threats.

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

AST-01: ASSET GOVERNANCE

Control Objective: The organization facilitates an IT Asset Management (ITAM) program to implement and manage asset management controls.[14]

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that includes, but is not limited to:

(a) Maintaining an accurate and current list of IT assets that includes but is not limited to:
    1. Make and model of the device;
    2. Location of device; and
    3. Device serial number or other methods of unique identification;
(b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices); and
(c) A list of company-approved products.

Guidelines: It is also possible that the owner and custodian of the hardware, software and data are the same, but this needs to be identified and documented.

AST-02: ASSET INVENTORIES

Control Objective: The organization performs inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:

(1) Accurately reflects the current TAASD in use;
(2) Identifies authorized software products, including business justification details;
(3) Is at the level of granularity deemed necessary for tracking and reporting;
(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and
(5) Is available for review and audit by designated organizational personnel.

Standard: ACME's Chief Information Officer (CIO), or the CIO's designated representative(s), must establish and maintain an IT Asset Management (ITAM) program that inventories ACME's Technology Assets, Applications, Services and/or Data (TAASD) as follows:

(a) Hardware and software inventories, both:
    1. Internally-hosted Technology Assets, Applications and/or Services (TAAS); and
    2. Externally-hosted TAAS;
(b) Sensitive/regulated data that is stored, processed and/or transmitted on the TAAS;
(c) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices);
(d) List of ACME-approved TAAS (e.g., software and hardware);
(e) Review and update inventories at least quarterly; and
(f) Where technically feasible, a list of all personnel with access to assets.

[14] *ISO 27001-2013: 4.2 | ISO 27002-2022: 5.30, 5.31, 7.9 | NIST SP 800-53 R5: PM-5 | NIST SP 800-171 R2: 3.4.1, 3.8.3 | NIST SP 800-171 R3: 03.01.03, 03.01.18.a, 03.04.11.a, 03.07.04.a| NIST CSF 2.0: GV.SC-04, ID.AM, ID.AM-08 | FAR 52.204-21(b)(1)(vii)*