YOUR LOGO GOES HERE

CORE FUNDAMENTALS POLICIES & STANDARDS

SECURE CONTROLS FRAMEWORK

CORE FUNDAMENTALS

ACME Business Operations, 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 Business Operations, LLP (ACME)'s systems, applications and services to protect its data, regardless of where it is stored, transmitted or processed. The following external content is a non-exhaustive list of frameworks that either support the implementation of or are referenced by the CORE Fundamentals:

- Secure Controls Framework (SCF)
  - Integrated Controls Management (ICM)[1]
  - Cybersecurity & Data Privacy Risk Management (C|P-RMM)[2]
  - Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM)[3]
  - Unified Scoping Guide (USG)[4]
- The National Institute of Standards and Technology (NIST): [5]
  - 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 IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- The International Organization for Standardization (ISO):[6]
  - ISO/IEC 15288: *Systems and Software Engineering -- System Life Cycle Processes*
  - ISO/IEC 22301: *Societal Security – Business Continuity Management Systems – Requirements*
- Other influencing frameworks (alphabetical order):
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)[7]
  - Computer Security Incident Handling Guide[8]
  - Defense Information Systems Agency (DISA) Secure Technology Implementation Guides (STIGs)[9]
  - Guide to Integrating Forensic Techniques into Incident Response[10]
  - Open Web Application Security Project (OWASP)[11]
  - Payment Card Industry Data Security Standard (PCI DSS)[12]

[1] *ICM - https://securecontrolsframework.com/free/integrated-controls-management/*
[2] *C|P-RMM - https://securecontrolsframework.com/free/risk-management-model/*
[3] *C|P-CMM - https://securecontrolsframework.com/free/capability-maturity-model/*
[4] *USG - https://securecontrolsframework.com/free/unified-scoping-guide*
[5] *National Institute of Standards and Technology - https://csrc.nist.gov/publications/sp*
[6] *International Organization for Standardization - https://www.iso.org/home.html*
[7] *Cloud Security Alliance - https://cloudsecurityalliance.org/*
[8] *Computer Security Incident Handling Guide - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final*
[9] *DoD Information Security Agency - https://public.cyber.mil/*
[10] *Guide to Integrating Forensic Techniques into Incident Response - https://csrc.nist.gov/publications/detail/sp/800-86/final*
[11] *OWASP - https://owasp.org/*
[12] *Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/*

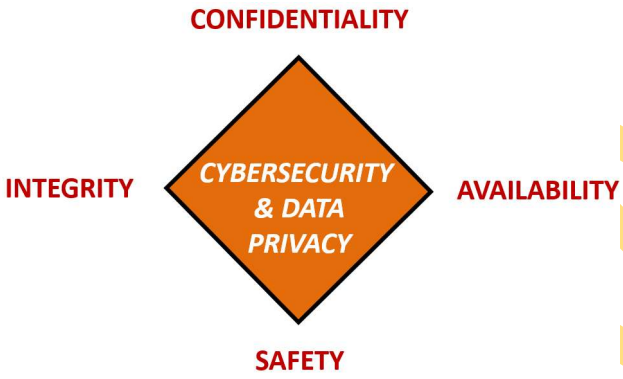
MANAGEMENT COMMITMENT

The Secure Controls Framework (SCF) created the Cybersecurity Oversight, Resilience and Enablement (CORE) initiative to help organizations tailor cybersecurity and data protection controls to fit its specific needs. The **SCF CORE Fundamentals** is a tailored set of sixty-eight (68) controls that are specifically designed for Small and Medium Businesses (SMB) to protect People, Processes, Technologies, Data and Facilities (PPTDF) against common threats.

The **CORE Fundamentals Policies & Standards** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Business Operations, 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 data and systems, applications and services. 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 & data privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



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

PURPOSE

The purpose of the CORE Fundamentals Policies & Standards is to:

- Identify and protect against reasonable threats to People, Processes, Technologies, Data and Facilities (PPTDF);
- Implement appropriate administrative, technical, and physical safeguards for the protection of sensitive / regulated data, including personal identifying information and sensitive personal information;
- 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.

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

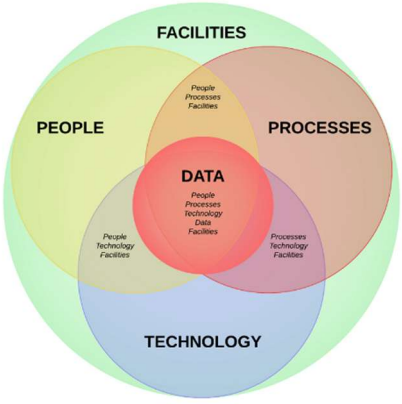
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual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

MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION

The objective is to provide management direction and support for cybersecurity and data protection in accordance with business requirements and relevant laws and regulations. [21]

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind ACME's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

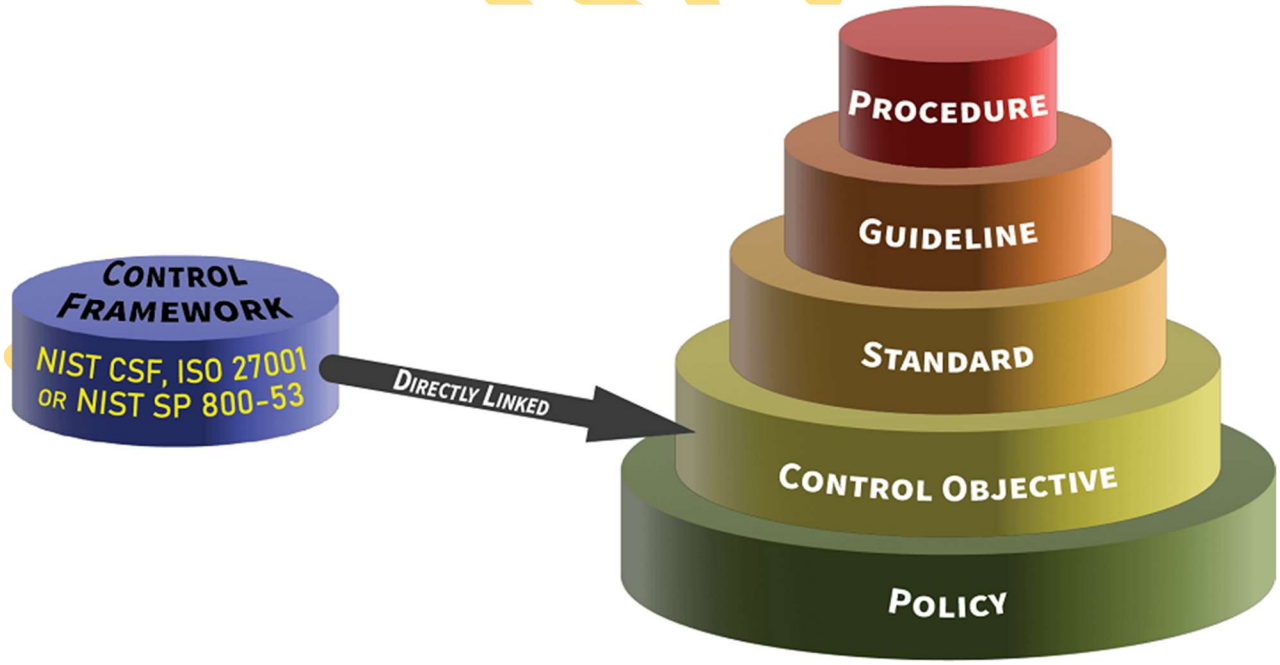
In accordance with leading practices, ACME's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA) or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

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

(1) Policy that establishes management's intent;
(2) Control Objective that identifies leading practices (linked to controls);
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.



[21] *ISO 27002:2013 5.1*

Management Intent: The purpose of the Asset Management (AST) policy is to ensure that technology assets 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 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.[26]

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 that: [27]

(1) Accurately reflects the current systems, applications and services 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 as follows:

(a) Hardware and software inventories, both:
    1. Internally-hosted assets; and
    2. Externally-hosted assets;
(b) A method to accurately and readily determine owner, contact information and purpose (e.g., labeling, coding and/or inventorying of devices);
(c) List of ACME-approved technology assets (e.g., software and hardware);
(d) Review and update inventories at least quarterly; and
(e) Where technically feasible, a list of all personnel with access to assets.

Guidelines: System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components

[26] *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 | NIST SP 800-171 R3: 03.01.03 | NIST CSF 2.0: GV.SC-04, ID.AM, ID.AM-08 | FAR 52.204-21(b)(1)(vii)*
[27] *ISO 27002-2022: 5.9 | NIST SP 800-53 R5: CM-8, PM-5 | NIST SP 800-171 R2: 3.4.1 | NIST SP 800-171 R3: 03.04.08.a, 03.04.08.c, 03.04.10.a, 03.04.10.b, 03.04.11.a | NIST CSF 2.0: ID.AM, ID.AM-01, ID.AM-02*

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

Policy: 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 on a production network.

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

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of change management controls. [35]

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 system, application and/or service must:

(a) Be:
    1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;
    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.

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

[35] *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*

- SUPPLEMENTAL DOCUMENTATION -

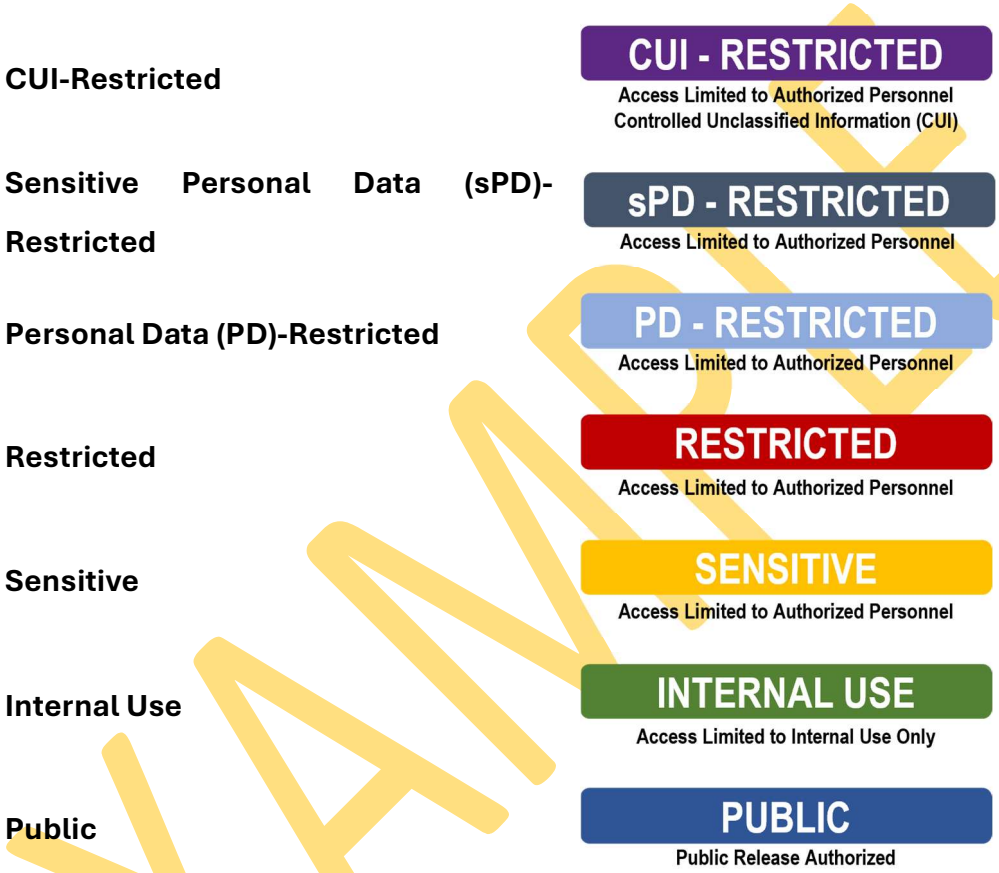
ANNEXES, TEMPLATES & REFERENCES

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.

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		