Your Logo
Will Be
Placed Here

CYBERSECURITY AND DATA PROTECTION PROGRAM (CDPP)

ISO 27001/27002:2013

ACME Business Consulting, LLC

CDPP
Cybersecurity & Data Protection Program

Table of Contents

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Business Consulting, LLC (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 Cybersecurity and Data Protection Program (CDPP):

- The International Organization for Standardization (**ISO**):[1]
  - 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*
- The National Institute of Standards and Technology (**NIST**): [2]
  - 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 800-64: *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)
- Other influencing frameworks (alphabetical order):
  - Center for Internet Security (**CIS**) Critical Security Controls (**CSC**)[3]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[4]
  - Fair Information Practice Principles (**FIPP**)[5]
  - Generally Accepted Privacy Practices (**GAPP**)[6]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[7]

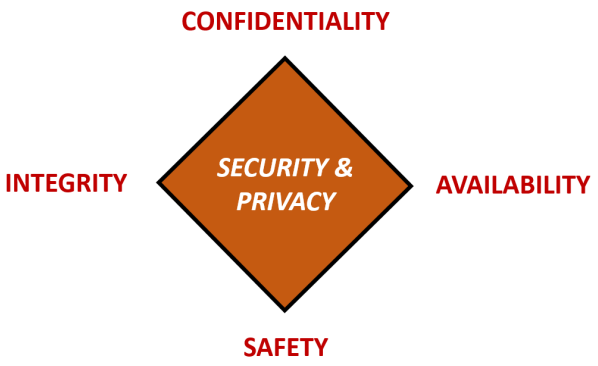
[1] International Organization for Standardization - https://www.iso.org
[2] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[3] Center for Internet Security - https://www.cisecurity.org/
[4] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[5] Federal Trade Commission - https://www.ftc.gov
[6] The American Institute of CPAs - http://www.aicpa.org
[7] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

INTRODUCTION

The **Cybersecurity and Data Protection Program (CDPP)** provides definitive information on the prescribed measures used to establish and enforce the security program at ACME Business Consulting, LLC (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, security and 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** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

PURPOSE

The purpose of the Cybersecurity and Data Protection Program (CDPP) is to prescribe a comprehensive framework for:

- Creating an Information Security Management System (ISMS) in accordance with ISO 27001.
- Protecting the confidentiality, integrity and availability of ACME data and information systems.
- Protecting ACME, its employees and its clients from illicit use of ACME information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support ACME's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Information Security risks.
- Providing for development, review and maintenance of minimum security controls required to protect ACME's data and information 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 users understand their day-to-day security responsibilities and the threats that could impact the company.

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. [12]

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

ACME's cybersecurity and data protection documentation is comprised of five (5) core components:

(1) Policies are established by ACME's corporate leadership establishes "management's intent" for cybersecurity and data protection requirements that are necessary to support ACME's overall strategy and mission;
(2) Controls / Control Objectives identify the technical, administrative and physical protections that are generally tied to a law, regulation, industry framework or contractual obligation;
(3) Standards provide ACME-specific, quantifiable requirements for cybersecurity and data protection;
(4) Procedures (also known as Control Activities) establish the defined practices or steps that are performed to meet to implement standards and satisfy controls / control objectives; and
(5) Guidelines are additional guidance that is recommended, but not mandatory.

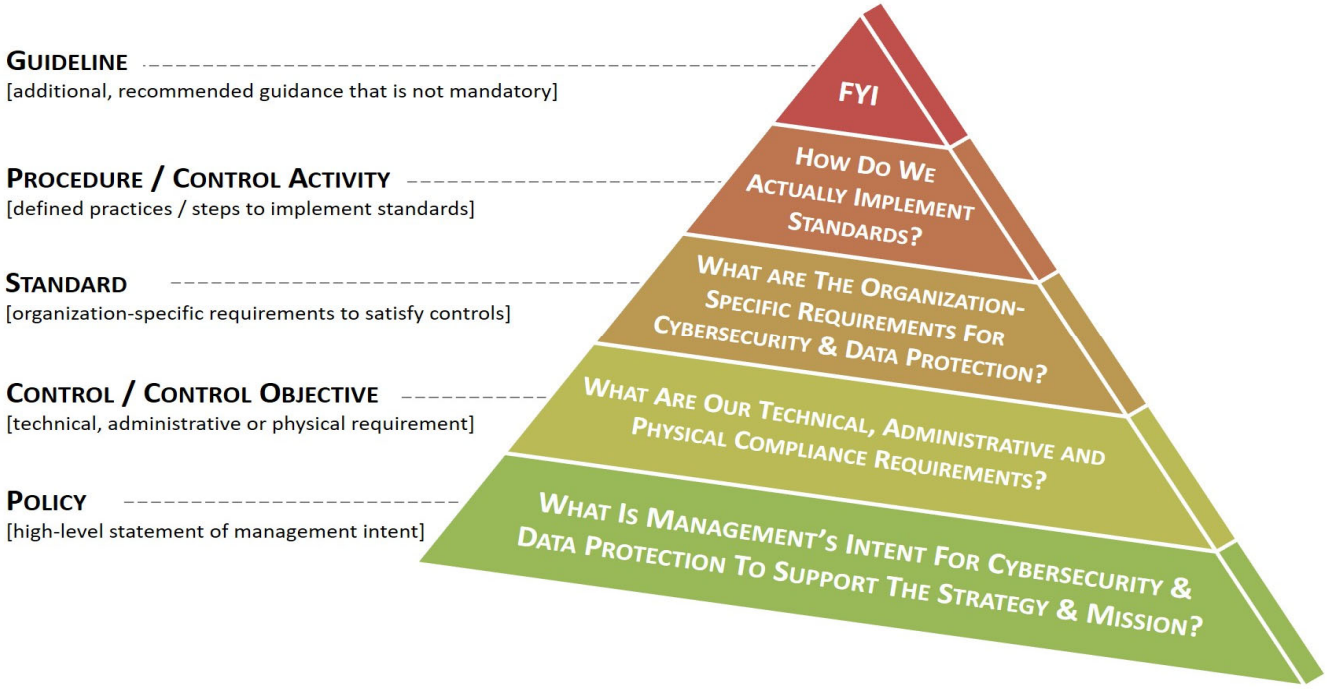


Figure 1: Cybersecurity & Data Protection Documentation Structure

[12] ISO 27002:2013 5.1

Management Intent: The purpose of the Security & Privacy Governance (GOV) policy is to specify the development, proactive management and ongoing review of ACME's security and privacy program.

Policy: ACME shall protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored. Digital 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, in accordance with all statutory, regulatory and contractual obligations.

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

GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control Objective: The organization facilitates the implementation of cybersecurity and privacy governance controls.[13]

Standard: ACME's security program shall be represented in a single document, the Cybersecurity and Data Protection Program (CDPP) that:

(a) Shall 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 privacy-related controls employed within the organization.

GOV-02: STEERING COMMITTEE

Control Objective: The organization coordinates cybersecurity, privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.[14]

Standard: ACME shall establish a cybersecurity and privacy 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;
(b) Receives briefings from the following:
    1. Chief Information Security Officer (CISO) on matters of cybersecurity;
    2. Chief Privacy Officer (CPO) on matters of privacy; and
    3. Chief Risk Officer (CRO) on matters of enterprise risk.

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

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

GOV-03: PUBLISHING SECURITY & PRIVACY POLICIES

Control Objective: The organization establishes, maintains and disseminates cybersecurity and privacy policies, standards and procedures. [15]

Standard: ACME's security and privacy policies and standards shall be represented in a consolidated document, the Cybersecurity and Data Protection Program (CDPP) that is:

(a) Endorsed by executive management; and

[13] ISO 27001: 5.1, 6.1.1 | ISO 27002: 5.1.1 | NIST SP 800-53 R5: PM-1
[14] ISO 27001: 6.2, 7.4, 9.3, 10.2
[15] ISO 27001: 5.2, 7.5.1, 7.5.2, 7.5.3 | ISO 27002: 5.1.1 | NIST SP 800-53 R5: PM-1 | NIST CSF: ID.GV-1

(b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

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

GOV-04: Periodic Review & Update of Security & Privacy Documentation

Control Objective: The organization reviews the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. [16]

Standard: ACME's business leadership (or other accountable business role or function) shall review the Cybersecurity and Data Protection Program (CDPP) at planned intervals or as a result of changes to the organization (e.g., mergers, acquisitions, partnerships, new products, etc.) to ensure its continuing alignment with the security strategy, risk posture, effectiveness, accuracy, relevance and applicability to statutory, regulatory and / or contractual compliance obligations.

Guidelines: Updates to the CDPP will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

GOV-05: Assigned Security & Privacy Responsibilities

Control Objective: The organization assigns a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.[17]

Standard: Executive and line management shall take formal action to support cybersecurity through clearly-documented direction and commitment and shall ensure the action has been assigned. The overall authority and responsibility for managing the security program are delegated to ACME's Chief Information Security Officer (CISO) and he / she is required to perform or delegate the following security management responsibilities:

(a) Establish, document and distribute security policies and procedures;
(b) Monitor and analyze security alerts and information;
(c) Distribute and escalate security alerts to appropriate personnel;
(d) Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations;
(e) Administer user accounts, including additions, deletions and modifications; and
(f) Monitor and control all access to data.

Guidelines: Central management refers to the organization-wide management and implementation of selected cybersecurity controls and related processes. Central management includes planning, implementing, assessing, authorizing and monitoring the organization-defined, centrally managed security controls and processes. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring.

GOV-06: Measures of Performance

Control Objective: The organization develops, reports and monitors cybersecurity and privacy program measures of performance.[18]

Standard: The Chief Information Security Officer (CISO) is assigned the responsibility for:

(a) Developing measures of performance or outcome-based metrics to measure the effectiveness or efficiency of the security program and security and privacy controls employed in support of the program;
(b) Communicating awareness and understanding of IT objectives and direction to appropriate stakeholders and users throughout the enterprise; and
(c) Sharing the effectiveness of protection technologies with appropriate parties.

[16] ISO 27001: 6.1.1, 7.4 | ISO 27002: 5.1.2 | NIST SP 800-53 R5: PM-1
[17] ISO 27001: 5.3 | NIST SP 800-53 R5: PL-9, PM-2, PM-6, PM-29 | NIST CSF: ID.AM-6
[18] ISO 27001: 9.1 | NIST SP 800-53 R5: PM-6 | NIST CSF: PR.IP-8

Management Intent: The purpose of the Configuration Management (CFG) policy is to establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced.

Policy: All technology platforms must adhere to configuration management requirements. ACME shall maintain accurate inventories of its technology platforms and enforce security configuration settings those technology platforms used in support of ACME's business operations.

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

CFG-01: CONFIGURATION MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of configuration management controls.[55]

Standard: ACME is required to document organization-wide configuration management controls that, at a minimum, include:

(a) A formal, documented configuration management program;
(b) Processes to facilitate the implementation of the configuration management program, including procedures and associated controls; and
(c) Where technically feasible, asset custodians and data / process owners must configure systems to include a description of groups, roles and responsibilities for the logical management of those devices.

Guidelines: As systems continue through the Secure Development Life Cycle (SDLC), new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Configuration management plans satisfy the requirements in organizational configuration management policies while being tailored to individual systems.

CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS

Control Objective: The organization develops, documents and maintains secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.[56]

Standard: Baseline security requirements shall be established for all ACME owned or managed assets that comply with applicable legal, statutory and regulatory compliance obligations:

(a) Each operating system shall be hardened to provide only necessary ports, protocols and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring and logging as part of their baseline operating build standard or template;
(b) Deviations from standard baseline configurations must be authorized following change management processes prior to deployment, provisioning or use; and
(c) Unless a technical or business reason exists, standardized images will be used to represent hardened versions of the underlying operating system and the applications installed on the system. These images must be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
(d) Data/process owners and asset custodians must develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to:
    1. Verifying that system configuration standards are:
        i. Updated as new vulnerability issues are identified;
        ii. Applied when new systems are configured;
        iii. Consistent with industry-accepted hardening standards;
    2. Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers and DNS should be implemented on separate servers);
    3. Enforcing least functionality, which includes but is not limited to:

[55] ISO 27002: 9.4.1 | NIST SP 800-53 R5: CM-1, CM-9 | NIST SP 800-171 R2: NFO - CM-1, NFO - CM-9
[56] ISO 27002: 9.4.1, 14.1.1 | NIST SP 800-53 R5: CM-2, CM-6, SA-8, PL-10, SA-15(5) | NIST CSF: PR.IP-1, PR.IP-3 | NIST SP 800-171 R2: 3.4.2

i. Allowing only necessary and secure services, protocols and daemons;
ii. Removing all unnecessary functionality, which includes but is not limited to:
    I. Scripts;
    II. Drivers;
    III. Features;
    IV. Subsystems;
    V. File systems; and
    VI. Unnecessary web servers
iii. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS) or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet and FTP;
iv. Verifying system security parameters are configured to prevent misuse; and
v. Documenting the functionality present on systems.

Guidelines: Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) [57]

Technology platforms includes but are not limited to:

- Firewalls;
- Routers;
- Switches, capable of being managed;
- Wireless Access Points (WAPs);
- Servers;
- Workstations;
- Embedded devices; and
- Mobile Devices, capable of being managed.

CFG-03: LEAST FUNCTIONALITY

Control Objective: The organization configures systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.[58]

Standard: ACME utilizes the "principle of least privilege,"[59] which states that only the minimum access and functionality necessary to perform an operation should be granted and only for the minimum amount of time necessary. Data/process owners and asset custodians must:

(a) Identifying and removing insecure services, protocols and ports;
(b) Enabling only necessary and secure services, protocols and daemons, as required for the function of the system;
(c) Implementing security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBIOS, Telnet, FTP, etc.);
(d) Verifying services, protocols and ports are documented and properly implemented by examining firewall and router configuration settings; and
(e) Removing all unnecessary functionality, such as:
    1. Scripts;
    2. Drivers;
    3. Features;
    4. Subsystems;
    5. File systems; and
    6. Unnecessary web servers.

[57] DISA STIGs official site: https://public.cyber.mil/
[58] ISO 27002: 9.4.1 | NIST SP 800-53 R5: CM-7 | NIST CSF: PR.PT-3 | NIST SP 800-171 R2: 3.4.6 | FAR: 52.204-21(b)(1)(ii)
[59] Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." Proceedings of the IEEE 63, 9 (September 1975): 1278-1308.

- SUPPLEMENTAL DOCUMENTATION -

CYBERSECURITY & DATA PROTECTION PROGRAM (CDPP)

ANNEXES, TEMPLATES & REFERENCES

Version 2021.1

CDPP
Cybersecurity & Data Protection Program

TABLE OF CONTENTS

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal 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 [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by [Company Name]
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name].
		· Impact could include negatively affecting [Company Name]'s competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by [Company Name], 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 [Company Name].
		· 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 [Company Name].
		· Impact would not be damaging or a risk to business operations.

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Confidential	Restricted
Client or Employee Personal Data	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
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	

ANNEX 3: DATA RETENTION PERIODS

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).*

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to [Company Name], its clients, its partners, or the general public.

The three (3) SC ratings are:

- SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of [Company Name]:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on [Company Name]'s mission.
    - Cannot go down without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of [Company Name]'s business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on [Company Name]'s mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- SC-3: Non-Critical. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on [Company Name]'s mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

Basic Assurance Requirements

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to [Company Name].