# TABLE OF CONTENTS

**Notice**  
Referenced Frameworks & Supporting Practices  
NIST 800-171 Compliance Program Overview  
Cybersecurity Program Structure  
Access Control (AC) Policy & Standards  
Audit & Accountability (AA) Policy & Standards

## Notice

7

## Referenced Frameworks & Supporting Practices

7

## NIST 800-171 Compliance Program Overview

8

- Introduction
- Purpose
- Scope & Applicability
- Policy Overview
- Violations
- Exceptions
- Updates
- Key Terminology

## Cybersecurity Program Structure

12

- Management Direction for Cybersecurity
- Documentation Hierarchy

## Access Control (AC) Policy & Standards

13

- **AC-01: Account Management**
- **AC-02: Access Enforcement**
- **AC-03: Data Flow Enforcement – Access Control Lists (ACLs)**
- **AC-04: Least Privilege**
- **AC-05: Authorize Access to Security Functions**
- **AC-06: Privileged Accounts**
- **AC-07: Non-Privileged Access for Non-Security Functions**
- **AC-08: Auditing Use of Privileged Functions**
- **AC-09: Prohibit Non-Privileged Users from Executing Privileged Functions**
- **AC-10: Account Lockout**
- **AC-11: System Use Notification (Logon Banner)**
- **AC-12: Session Lock**
- **AC-13: Pattern-Hiding Displays**
- **AC-14: Session Termination**
- **AC-15: Automated Monitoring & Control**
- **AC-16: Protection of Confidentiality / Integrity Using Encryption**
- **AC-17: Managed Access Control Points**
- **AC-18: Privileged Commands & Access**
- **AC-19: Wireless Networking**
- **AC-20: Authentication & Encryption**
- **AC-21: Access Control for Mobile Devices**
- **AC-22: Full Device & Container-Based Encryption**
- **AC-23: Use of External Information Systems**
- **AC-24: Limits of Authorized Use**
- **AC-25: Portable Storage Devices**
- **AC-26: Publicly Accessible Content**

## Audit & Accountability (AA) Policy & Standards

23

- **AA-01: Continuous Monitoring**
- **AA-02: Inbound & Outbound Communications Traffic**
- **AA-03: Centralized Event Log Collection**
- **AA-04: System Generated Alerts**
- **AA-05: Content of Audit Records**
- **AA-06: Monitoring Reporting**
- **AA-07: Sensitive Audit Information**
- **AA-08: Audit Record Retention**
- **AA-09: Reviews & Updates**
- **AA-10: Response To Audit Processing Failures**
- **AA-11: Correlate Monitoring Information**
AA-12: TIME STAMPS
AA-13: SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
AA-14: PROTECTION OF AUDIT INFORMATION
AA-15: ACCESS BY SUBSET OF PRIVILEGED USERS

AWARENESS & TRAINING (AT) POLICY & STANDARDS
AT-01: SECURITY & PRIVACY-MINDED WORKFORCE
AT-02: SECURITY & PRIVACY AWARENESS
AT-03: SECURITY & PRIVACY TRAINING
AT-04: TRAINING RECORDS
AT-05: INSIDER THREAT AWARENESS

CONFIGURATION MANAGEMENT (CM) POLICY & STANDARDS
CM-01: CONFIGURATION MANAGEMENT PROGRAM
CM-02: ASSET INVENTORIES
CM-03: UPDATES DURING INSTALLATIONS / REMOVALS
CM-04: COMPONENT DUPLICATION AVOIDANCE
CM-05: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS
CM-06: REVIEWS & UPDATES
CM-07: CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS
CM-08: CONFIGURATION CHANGE CONTROL
CM-09: TEST, VALIDATE & DOCUMENT CHANGES
CM-10: SECURITY REPRESENTATIVE FOR CHANGE
CM-11: SECURITY IMPACT ANALYSIS FOR CHANGES
CM-12: ACCESS RESTRICTION FOR CHANGE
CM-13: STAKEHOLDER NOTIFICATION OF CHANGES
CM-14: LEAST FUNCTIONALITY
CM-15: PERIODIC REVIEW
CM-16: PREVENT PROGRAM EXECUTION
CM-17: UNAUTHORIZED OR AUTHORIZED SOFTWARE (BLACKLISTING OR WHITELISTING)
CM-18: USER-INSTALLED SOFTWARE

CYBERSECURITY GOVERNANCE (CG) POLICY & STANDARDS
CG-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE
CG-02: SECURITY PORTFOLIO MANAGEMENT
CG-03: ALLOCATION OF RESOURCES
CG-04: SECURE DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT

IDENTIFICATION & AUDIT (IA) POLICY & STANDARDS
IA-01: IDENTITY & ACCESS MANAGEMENT (IAM)
IA-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS
IA-03: IDENTIFICATION & AUTHENTICATION FOR DEVICES
IA-04: AUTHENTICATOR MANAGEMENT (PASSWORDS)
IA-05: MULTI-FACTOR AUTHENTICATION (MFA) - NETWORK ACCESS TO PRIVILEGED ACCOUNTS
IA-06: MULTI-FACTOR AUTHENTICATION (MFA) - NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS
IA-07: MULTI-FACTOR AUTHENTICATION (MFA) - LOCAL ACCESS TO PRIVILEGED ACCOUNTS
IA-08: NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT
IA-09: IDENTIFIER MANAGEMENT (USER NAMES)
IA-10: PASSWORD-BASED AUTHENTICATION
IA-11: PROTECTION OF AUTHENTICATORS
IA-12: AUTHENTICATOR FEEDBACK

INCIDENT RESPONSE (IR) POLICY & STANDARDS
IR-01: INCIDENTS RESPONSE OPERATIONS
IR-02: INCIDENT HANDLING
IR-03: INCIDENT RESPONSE PLAN (IRP)
IR-04: IRP UPDATE
IR-05: INCIDENT MONITORING & TRACKING
IR-06: INCIDENT REPORTING ASSISTANCE
IR-07: INCIDENT RESPONSE TRAINING
IR-08: INCIDENT REPORTING
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-09</td>
<td>INCIDENT RESPONSE TESTING</td>
<td>50</td>
</tr>
<tr>
<td>IR-10</td>
<td>ROOT CAUSE ANALYSIS (RCA) &amp; LESSONS LEARNED</td>
<td>50</td>
</tr>
<tr>
<td><strong>MAINTENANCE (MT) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>MA-01</td>
<td>MAINTENANCE OPERATIONS</td>
<td>51</td>
</tr>
<tr>
<td>MA-02</td>
<td>CONTROLLED MAINTENANCE</td>
<td>51</td>
</tr>
<tr>
<td>MA-03</td>
<td>MAINTENANCE TOOLS</td>
<td>52</td>
</tr>
<tr>
<td>MA-04</td>
<td>INSPECT TOOLS</td>
<td>52</td>
</tr>
<tr>
<td>MA-05</td>
<td>INSPECT MEDIA</td>
<td>52</td>
</tr>
<tr>
<td>MA-06</td>
<td>NON-LOCAL MAINTENANCE</td>
<td>52</td>
</tr>
<tr>
<td>MA-07</td>
<td>NOTIFICATION OF NON-LOCAL MAINTENANCE</td>
<td>53</td>
</tr>
<tr>
<td>MA-08</td>
<td>MAINTENANCE PERSONNEL</td>
<td>53</td>
</tr>
<tr>
<td><strong>MEDIA PROTECTION (MP) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>54</td>
</tr>
<tr>
<td>MP-01</td>
<td>DATA PROTECTION</td>
<td>54</td>
</tr>
<tr>
<td>MP-02</td>
<td>MEDIA ACCESS</td>
<td>54</td>
</tr>
<tr>
<td>MP-03</td>
<td>MEDIA STORAGE</td>
<td>54</td>
</tr>
<tr>
<td>MP-04</td>
<td>DIGITAL MEDIA SANITIZATION</td>
<td>55</td>
</tr>
<tr>
<td>MP-05</td>
<td>MEDIA MARKING</td>
<td>55</td>
</tr>
<tr>
<td>MP-06</td>
<td>MEDIA TRANSPORTATION</td>
<td>56</td>
</tr>
<tr>
<td>MP-07</td>
<td>TRANSMISSION INTEGRITY</td>
<td>56</td>
</tr>
<tr>
<td>MP-08</td>
<td>MEDIA USE</td>
<td>56</td>
</tr>
<tr>
<td>MP-09</td>
<td>DATA BACKUPS</td>
<td>56</td>
</tr>
<tr>
<td><strong>PERSONNEL SECURITY (PS) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>58</td>
</tr>
<tr>
<td>PS-01</td>
<td>HUMAN RESOURCES SECURITY MANAGEMENT</td>
<td>58</td>
</tr>
<tr>
<td>PS-02</td>
<td>ACCESS AGREEMENTS</td>
<td>58</td>
</tr>
<tr>
<td>PS-03</td>
<td>SEPARATION OF DUTIES</td>
<td>58</td>
</tr>
<tr>
<td>PS-04</td>
<td>PERSONNEL SCREENING</td>
<td>59</td>
</tr>
<tr>
<td>PS-05</td>
<td>PERSONNEL TRANSFER</td>
<td>59</td>
</tr>
<tr>
<td>PS-06</td>
<td>PERSONNEL SANCTIONS</td>
<td>59</td>
</tr>
<tr>
<td>PS-07</td>
<td>PERSONNEL TERMINATION</td>
<td>59</td>
</tr>
<tr>
<td>PS-08</td>
<td>RULES OF BEHAVIOR</td>
<td>60</td>
</tr>
<tr>
<td>PS-09</td>
<td>SOCIAL MEDIA &amp; SOCIAL NETWORKING RESTRICTIONS</td>
<td>61</td>
</tr>
<tr>
<td>PS-10</td>
<td>THIRD-PARTY PERSONNEL SECURITY</td>
<td>61</td>
</tr>
<tr>
<td><strong>PHYSICAL PROTECTION (PP) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>62</td>
</tr>
<tr>
<td>PP-01</td>
<td>PHYSICAL &amp; ENVIRONMENTAL PROTECTIONS</td>
<td>62</td>
</tr>
<tr>
<td>PP-02</td>
<td>PHYSICAL ACCESS AUTHORIZATIONS</td>
<td>62</td>
</tr>
<tr>
<td>PP-03</td>
<td>PHYSICAL ACCESS LOGS</td>
<td>62</td>
</tr>
<tr>
<td>PP-04</td>
<td>MONITORING PHYSICAL ACCESS</td>
<td>63</td>
</tr>
<tr>
<td>PP-05</td>
<td>INTRUSION ALARMS / SURVEILLANCE EQUIPMENT</td>
<td>63</td>
</tr>
<tr>
<td>PP-06</td>
<td>ACCESS CONTROL FOR OUTPUT DEVICES</td>
<td>63</td>
</tr>
<tr>
<td>PP-07</td>
<td>ACCESS CONTROL FOR TRANSMISSION MEDIUM</td>
<td>64</td>
</tr>
<tr>
<td>PP-08</td>
<td>PHYSICAL ACCESS CONTROL</td>
<td>64</td>
</tr>
<tr>
<td>PP-09</td>
<td>ALTERNATE WORK SITE</td>
<td>65</td>
</tr>
<tr>
<td>PP-10</td>
<td>DELIVERY &amp; REMOVAL</td>
<td>65</td>
</tr>
<tr>
<td><strong>RISK ASSESSMENT (RA) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>66</td>
</tr>
<tr>
<td>RA-01</td>
<td>RISK MANAGEMENT PROGRAM</td>
<td>66</td>
</tr>
<tr>
<td>RA-02</td>
<td>RISK ASSESSMENT</td>
<td>66</td>
</tr>
<tr>
<td>RA-03</td>
<td>PRIVILEGED ACCESS</td>
<td>67</td>
</tr>
<tr>
<td>RA-04</td>
<td>VULNERABILITY SCANNING</td>
<td>67</td>
</tr>
<tr>
<td>RA-05</td>
<td>UPDATE TOOL CAPABILITY</td>
<td>68</td>
</tr>
<tr>
<td><strong>SECURITY ASSESSMENT (SA) POLICY &amp; STANDARDS</strong></td>
<td></td>
<td>69</td>
</tr>
<tr>
<td>SA-01</td>
<td>INFORMATION ASSURANCE (IA) OPERATIONS</td>
<td>69</td>
</tr>
<tr>
<td>SA-02</td>
<td>SECURITY ASSESSMENTS</td>
<td>69</td>
</tr>
<tr>
<td>SA-03</td>
<td>INDEPENDENT ASSESSORS</td>
<td>69</td>
</tr>
<tr>
<td>SA-04</td>
<td>SYSTEM SECURITY PLANS (SSP)</td>
<td>70</td>
</tr>
<tr>
<td>SA-05</td>
<td>PLAN OF ACTION &amp; MILESTONES (POA&amp;M)</td>
<td>70</td>
</tr>
</tbody>
</table>
SA-06: SECURITY CONTROLS OVERSIGHT
SA-07: PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

SERVICE PROVIDER (SP) POLICY & STANDARDS
SP-01: THIRD-PARTY MANAGEMENT
SP-02: THIRD-PARTY SERVICES
SP-03: IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS & SERVICES
SP-04: MANAGING CHANGES TO THIRD-PARTY SERVICES

SYSTEM & COMMUNICATIONS PROTECTION (SC) POLICY & STANDARDS
SC-01: SECURE ENGINEERING PRINCIPLES
SC-02: TECHNOLOGY LIFECYCLE MANAGEMENT
SC-03: ALIGNMENT WITH ENTERPRISE ARCHITECTURE
SC-04: NETWORK SECURITY MANAGEMENT
SC-05: REMOTE ACCESS
SC-06: BOUNDARY PROTECTION
SC-07: ACCESS POINTS
SC-08: EXTERNAL TELECOMMUNICATIONS SERVICES
SC-09: PARTITIONING
SC-10: INFORMATION IN SHARED RESOURCES
SC-11: DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION
SC-12: SYSTEM INTERCONNECTIONS
SC-13: INTERNAL SYSTEM CONNECTIONS
SC-14: SPLIT TUNNELING
SC-15: ALTERNATE PHYSICAL PROTECTION
SC-16: NETWORK DISCONNECT
SC-17: PUBLIC KEY INFRASTRUCTURE (PKI)
SC-18: USE OF CRYPTOGRAPHIC CONTROLS
SC-19: COLLABORATIVE COMPUTING DEVICES
SC-20: MOBILE CODE
SC-21: ELECTRONIC MESSAGING
SC-22: SESSION AUTHENTICITY
SC-23: ENDPOINT PROTECTION MEASURES
SC-24 DOMAİN NAME SERVICE (DNS) RESOLUTION
SC-25: ARCHITECTURE & PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
SC-26: SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
SC-27: PROCESS ISOLATION
SC-28: MEMORY PROTECTION

SYSTEM & INFORMATION INTEGRITY (SI) POLICY & STANDARDS
SI-01: THREAT INTELLIGENCE FEEDS
SI-02: SOFTWARE PATCHING
SI-03: MALICIOUS CODE PROTECTION (ANTI-MALWARE)

SYSTEM DEVELOPMENT (SD) POLICY & STANDARDS
SD-01: TECHNOLOGY DEVELOPMENT & ACQUISITION
SD-02: SECURITY REQUIREMENTS
SD-03: PORTS, PROTOCOLS & SERVICES IN USE
SD-04: USE OF APPROVED PIV PRODUCTS
SD-05: DOCUMENTATION REQUIREMENTS
SD-06: FUNCTIONAL PROPERTIES
SD-07: SECURE CODING
SD-08: SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT
SD-09: DEVELOPER CONFIGURATION MANAGEMENT

APPENDICES
APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES
A-1: DATA CLASSIFICATION
A-2: LABELING
A-3: GENERAL ASSUMPTIONS
A-4: SENSITIVE PERSONAL INFORMATION (SPI)
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 [Official Company Name] ([Company Name])’s systems, applications and services. The following external content is a non-exhaustive list of frameworks that are referenced by or support this NIST 800-171 Compliance Program (NCP):

- The National Institute of Standards and Technology (NIST):
  - NIST 800-39: Managing Cybersecurity Risk: Organization, Mission and Information System View
  - NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST 800-64: Security Considerations in Secure Development Life Cycle
  - NIST 800-122: Guide to Protecting the Confidentiality of Personal Information (PI)
  - NIST 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):
  - ISO 27002: Information Technology -- Security Techniques -- Code of Practice for Cybersecurity Controls
  - ISO 27018: Information Technology -- Security Techniques -- Code of Practice for Protection of Personal Information (PI) in Public Clouds Acting as PI Processors

- Other Frameworks:
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)
  - Center for Internet Security (CIS)
  - Department of Defense Cybersecurity Agency (DISA) Secure Technology Implementation Guides (STIGs)
  - Secure Controls Framework (SCF)

---

1 National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
2 International Organization for Standardization - https://www.iso.org
3 Cloud Security Alliance - https://cloudsecurityalliance.org/
4 Center for Internet Security - https://www.cisecurity.org/
NIST 800-171 COMPLIANCE PROGRAM OVERVIEW

INTRODUCTION

[Company Name] is committed to protecting its employees, partners, clients and [Company Name] from damaging acts that are intentional or unintentional. Effective cybersecurity is a team effort involving the participation and support of every [Company Name] user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company data and the systems that collect, process and maintain this information is of critical importance. Consequently, the security of systems 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 restricted 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.

Commensurate with risk, security measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction.

PURPOSE

The purpose of the NIST 800-171 Compliance Program (NCP) is to prescribe a comprehensive framework for:

- Creating a leading practice-based cybersecurity program to address NIST 800-171 requirements for:
  - Controlled Unclassified Information (CUI); and
  - Non-Federal Organization (NFO);
- Protecting the confidentiality, integrity, availability and safety of [Company Name] data and systems;
- Protecting [Company Name], its employees and its clients from illicit use of [Company Name] systems and data;
- Ensuring the effectiveness of security controls over data and systems that support [Company Name]’s operations.
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review and maintenance of minimum security controls required to protect [Company Name]’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 [Company Name] 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 [Company Name] users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help [Company Name] comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of [Company Name] data.
**SCOPE & APPLICABILITY**

The NCP provides definitive information on the prescribed measures used to establish and enforce the NIST 800-171 compliance program at [Official Company Name] ([Company Name]).

These policies, standards and procedures apply to all [Company Name]:

- Employees, contractors, sub-contractors and their respective facilities supporting [Company Name] business operations, wherever [Company Name] data is stored or processed, including any third-party contracted by [Company Name] to handle, process, transmit, store or dispose of [Company Name] data; and
- Data, systems, activities and assets owned, leased, controlled or used by [Company Name], its agents, contractors or other business partners on behalf of [Company Name] that are within scope of NIST 800-171 through storing, processing or transmitting Controlled Unclassified Information (CUI).

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting [Company Name] business functions shall comply with the standards. [Company Name] departments shall 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.

*Appendix E* (Cybersecurity Roles & Responsibilities) provides a detailed description of [Company Name] user roles and responsibilities, in regards to Information Security.

**POLICY OVERVIEW**

To ensure an acceptable level of cybersecurity risk, [Company Name] is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

[Company Name] users are required to 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**

Any [Company Name] 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.

**EXCEPTIONS**

While every exception to a standard potentially weakens protection mechanisms for [Company Name] systems and underlying data, occasionally exceptions will exist. When requesting an exception, users are required to submit a business justification for deviation from the standard in question.

**UPDATES**

[Company Name] reserves the right to revoke, change or supplement these policies, standards and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management unless otherwise stated.

Updates to the NCP 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.
KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the primary reference document that [Company Name] uses to define common cybersecurity terms. 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.

**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 [Company Name] 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.

**Cardholder Data Environment (CDE):** A term describing the area of the network that possesses sensitive data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage or transmission. Adequate network segmentation, which isolates systems that store, process or transmit sensitive data from those that do not, may reduce the scope of the sensitive data environment and thus the scope of the Payment Card Industry Data Security Standard (PCI DSS) assessment.

**Cloud Computing:** A term describing a 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, infrastructure-as-a-service and platform-as-a-service.

**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 [Company Name] accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

**Control Objective:** A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align [Company Name] with accepted due care requirements.

**Data:** A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. Appendix A (Data Classification & Handling Guidelines) provides guidance on data classification and handling restrictions.

**Data / Process Owner:** A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, process or the data hosted on the asset or process. It does not mean that the asset belongs to the owner in a legal sense. Data / process owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.

**Encryption:** A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

**Guidelines:** A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

**Information Security:** A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

**Information Technology (IT).** A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

---

7 NIST IR 7298 - [http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf](http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)
Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

Personal Data / Personal Information (PI). A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.8

PI Controller / Data Controller. A term describing the privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing Personal Information (PI) other than natural persons who use data for personal purposes

PI Principal / Data Principle. A term describing the natural person to whom the Personal Information (PI) relates

PI Processor / Data Processor. A term describing the privacy stakeholder that processes Personal Information (PI) on behalf of and in accordance with the instructions of a PI controller

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include sensitive Personal Information (sPI), Electronic Protected Health Information (ePHI) and all other forms of data classified as Restricted or Confidential in Appendix A (Data Classification & Handling Guidelines).

Sensitive Personal Data / Sensitive Personal Information (sPI): A term describing personal data, revealing:
- The first name or first initial and last name, in combination with any one or more of the following data elements:9
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN);
  - Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.);
  - Financial account number; or
  - Payment card number (e.g., credit or debit card);
- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade-union membership;
- Physical or mental health;
- Sex life and sexual orientation;
- Genetic data; and / or
- Biometric data.10

Standard: A term describing formally established requirements in regard to processes, actions and configurations.

System: A term describing an asset; a system or network that can be defined, scoped and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls and mobile devices.

Target Audience: A term describing the intended group for which a control or standard is directed.

---

8 European Union General Data Protection Requirement – Article 4(1)
9 The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - http://www.leg.state.or.us/ors/646a.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
10 European Union General Data Protection Requirement – Article 9(1)
**CYBERSECURITY PROGRAM STRUCTURE**

**MANAGEMENT DIRECTION FOR CYBERSECURITY**
The objective is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations.  

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind [Company Name]'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, [Company Name]'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.

**DOCUMENTATION HIERARCHY**
Cybersecurity documentation is comprised of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirement; procedures that must be followed; and guidelines that are recommended, but not mandatory.

Cybersecurity documentation is comprised of five main parts:

1. Core policy that establishes management’s intent;
2. Control objective that identifies the condition that should be met;
3. Standards that provides quantifiable requirements to be met;
4. Procedures that establish how tasks must be performed to meet the requirements established in standards; and
5. Guidelines are recommended, but not mandatory.

![Cybersecurity Documentation Hierarchy](image)

**Figure 1: Cybersecurity Documentation Hierarchy**

---

11 ISO 27002 5.1
ACCESS CONTROL (AC) POLICY & STANDARDS

Management Intent: The purpose of the Access Control (AC) policy is to implement the concept of “least privilege” through limiting access to [Company Name]’s systems and data to authorized users only.

Policy: [Company Name] shall implement the principle of “least privilege” within logical access control mechanisms so that only authorized users can gain access to [Company Name]’s systems and data.

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

AC-01: ACCOUNT MANAGEMENT

Control Objective: The organization manages system accounts, including:12

- Identifying account types (e.g., individual, group, system, application, guest / anonymous and temporary);
- Establishing conditions for group membership;
- Identifying authorized users of the system and specifying access privileges;
- Requiring appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling and removing accounts;
- Specifically authorizing and monitoring the use of guest / anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when system users are terminated, transferred or system usage or need-to-know / need-to-share changes;
- Deactivating accounts that are no longer required;
- Granting access to the system based on a valid access authorization; and
- Reviewing accounts on a regular basis.

Standard: [Company Name]’s IT department is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

(a) Control addition, deletion and modification of user IDs, credentials and other identifier objects to ensure authorized use is maintained;
(b) Verify user identity before issuing initial passwords or performing password resets;
(c) Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;
(d) Immediately revoke access for any terminated users;
(e) Remove / disable inactive user accounts within ninety (90) days;
(f) Limit repeated access attempts by locking out the user ID after not more than six (6) attempts;
(g) Set the lockout duration to a minimum of thirty (30) minutes or until administrator enables the user ID;
(h) Establish and administer accounts in accordance with a role-based access scheme that organizes system and network privileges into roles;
(i) Track and monitor role assignments for privileged user accounts;
(j) Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;
(k) Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;
(l) Minimize the use of group, shared or generic accounts and passwords;
(m) Disable or remove default user IDs and accounts;
(n) Service providers with remote access to [Company Name]’s premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password / phrase) for each customer; and
(o) Restrict user direct access or queries to databases to database administrators, including:

1. Verify that database and application configuration settings ensure that all user access to, user queries of and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);
2. Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators; and
3. Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

---

12 NIST 800-53 rev4 AC-2 | FedRAMP | NIST 800-171 3.1.1 & 3.1.2 | GAPP 8.2.2 | PCI DSS 8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 & 8.7 | MA201CMR17 17.04(1(a) | NIST CSF PR.AC-1 | CCM IAC-10 | NISPOM 8-607
Guidelines: Access privileges granted to general users should be reviewed by information owners every six (6) months to determine if access rights are commensurate with the user’s job duties:
- Evidence of account and privilege reviews that documents the review occurred, who conducted the review and what action (if any) was taken should be maintained for a period of twelve (12) months; and
- Asset custodians and data / process owners are required to promptly report all changes in user duties or employment status for the User IDs associated with the involved personnel and administrators should promptly revoke all unnecessary access privileges.

AC-02: ACCESS ENFORCEMENT
Control Objective: Systems enforce approved authorizations for logical access to the system in accordance with applicable policy.\(^\text{13}\)

Standard: [Company Name] is required to limit access to systems and sensitive data to only those individuals whose job requires such access.

Guidelines: The objective is to prevent unauthorized access to systems and applications. Access limitations should include the following:
- Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities;
- Assignment of privileges is based on individual personnel’s job classification and function;
- Requirement for a documented approval by authorized parties specifying required privileges; and
- Implementation of an automated access control system.

AC-03: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)
Control Objective: The organization builds firewall and router configurations that follow industry-recognized leading practices to restrict connections between untrusted networks and internal systems.\(^\text{14}\)

Standard: Network administrators are required to deploy and configure firewalls and routers in order to restrict connections between untrusted networks and any system components within the network by the following means:
(a) Implement Access Control Lists (ACLs) and other applicable filters to restrict the inbound and outbound traffic to only that which is necessary, as defined by a business justification;
(b) Assign privileges to individuals based on job classification and function (RBAC);
(c) Utilize “deny-all” setting by default and only allow by exception;
(d) Secure and synchronize router and firewall configuration files;
(e) Position perimeter firewalls between wireless networks and internal networks;
(f) Document business justification for the use if all services, protocols and ports allowed;
(g) Use Demilitarized Zones (DMZ) to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols and ports;
(h) Inbound Internet traffic shall be limited to IP addresses within the DMZ;
(i) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network;
(j) Prohibit unauthorized outbound traffic to the Internet;
(k) Implement stateful inspection (dynamic packet filtering);
(l) Segment internal trusted networks from other untrusted networks; and
(m) Prohibit private IP addresses and routing information from being disclosed to unauthorized parties.
(n) Establish and maintain a formal process for approving and testing all network connections and changes to both firewall and router configurations;
(o) Establish and maintain detailed network diagrams. Network diagrams must:
1. Document all connections to sensitive data, including any wireless networks;
2. Be reviewed annually; and
3. Be updated as the network changes to reflect the current architecture in place;
(p) Establish and maintain detailed data flow diagrams that show all sensitive data flows across systems and networks;
(q) Establish a process to review configurations at least once every six (6) months and cover the following:
   1. Validation of Access Control Lists (ACLs); and

\(^{13}\) NIST 800-53 rev4 AC-3 | ISO 27002 9.2.6 & 9.4 | FedRAMP | NIST 800-171 3.1.1 & 3.1.2 | PCI DSS 7.1-7.1.4, 7.2, 7.2.1 & 7.2.3 | MA201CMR17 17.04(1)(b) & 17.04(2)(a) | OR646A 622(2)(d)(C)(iii) | NISPOM 8-607

\(^{14}\) NIST 800-53 rev4 AC-4 & AU-8 | ISO 27002 9.4.1, 13.1.1 & 14.1.2 | FedRAMP | NIST 800-171 3.1.3 | PCI DSS 1.1-1.1.7, 1.2-1.2.3, 1.3.3, 1.3.5 & 7.2-7.2.3 | OR646A 622(2)(d)(C)(iii)
2. Vulnerability management (e.g., validating software and firmware is current).

**Guidelines:** Not all firewalls and routers have the functionality for the running configuration to be different that the configuration loaded at startup. However, if the functionality exists, the startup configuration must be synchronized with the correct running configuration so that a reboot of the device will not degrade network security.

Examples of insecure services, protocols or ports include but are not limited to:
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP)

**AC-04: LEAST PRIVILEGE**

**Control Objective:** The organization employs the concept of least privilege, allowing only authorized accesses for users and processes which are necessary to accomplish assigned tasks in accordance with organizational business functions.\(^{15}\)

**Standard:** [Company Name] follows the “principle of least privilege,”\(^{16}\) which states that only the minimum access necessary to perform an operation should be granted. Access will be granted only for the minimum:
- (a) Levels of permissions necessary to perform the job function; and
- (b) Time required.

**Guidelines:** [Company Name] employs the concept of least privilege for specific duties and systems (including specific functions, ports, protocols and services). The concept of least privilege is also applied to system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions. [Company Name] considers the creation of additional processes, roles and system accounts as necessary to achieve least privilege. [Company Name] also applies least privilege concepts to the design, development, implementation and operations of systems.

**AC-05: AUTHORIZE ACCESS TO SECURITY FUNCTIONS**

**Control Objective:** The organization explicitly authorizes access to organization-defined security functions (deployed in hardware, software and firmware) and security-relevant information.\(^{17}\)

**Standard:** Only explicitly-authorized personnel are permitted to have access to security functions and security-related information.

**Guidelines:** Security functions include, for example, establishing system accounts, configuring access authorizations (e.g., permissions, privileges), setting events to be audited and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers and other privileged users.

**AC-06: PRIVILEGED ACCOUNTS**

**Control Objective:** The organization restricts privileged accounts to organization-defined personnel or roles.\(^{18}\)

**Standard:** Assignment of privileged accounts must be limited to users who have:
- (a) A valid business justification;
- (b) Received security awareness training commensurate with the level of risk from having privileged access; and
- (c) Demonstrated technical competence specific to the environment where privileged access is being granted.

---

\(^{15}\) NIST 800-53 rev4 AC-6 | ISO 27002 9.1.2 | FedRAMP | NIST 800-171 3.1.5 | OR646A 622(2)(d)(C)(iii) | NIST CSF PR.AC-4 | SOC2 CC5.6 | ENISA SO11 | NISPOM 8-303


\(^{17}\) NIST 800-53 rev4 AC-6(1) | FedRAMP | NIST 800-171 3.1.5

\(^{18}\) NIST 800-53 rev4 AC-6(5) | FedRAMP | NIST 800-171 3.1.5
Guidelines: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information / functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided that organizations retain the ability to control information.

Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux / UNIX, “run as” on Windows and other similar facilities for other types of systems.

**AC-07: NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS**

**Control Objective:** The organization requires that users of system accounts or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts or roles, when accessing non-security functions. 19

**Standard:** Users must use accounts with the least privileges necessary to perform their job functions and are therefore prohibited from using privileged accounts to perform non-privileged functions.

**Guidelines:** This standard limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

**AC-08: AUDITING USE OF PRIVILEGED FUNCTIONS**

**Control Objective:** Systems audit the execution of privileged functions. 20

**Standard:** [Company Name] is required to establish a process for linking all access to systems, including administrative privileged accounts (e.g., root or administrator) to each individual user.

**Guidelines:** Misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and in doing so, help mitigate the risk from insider threats and Advanced Persistent Threats (APT).

**AC-09: PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS**

**Control Objective:** Systems prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures. 21

**Standard:** Where technically feasible, systems must be configured to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.

**Guidelines:** Privileged functions include, for example, establishing system accounts, performing system integrity checks or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

**AC-10: ACCOUNT LOCKOUT**

**Control Objective:** Systems: 22

- Enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period; and
- Automatically lock the account when the maximum number of unsuccessful attempts is exceeded.

---

19 NIST 800-53 rev4 AC-6(2) | FedRAMP | NIST 800-171 3.1.6 | CSC 5.8
20 NIST 800-53 rev4 AC-6(9) | FedRAMP | NIST 800-171 3.1.7 | PCI DSS 10.2-10.2.7
21 NIST 800-53 rev4 AC-6(10) | FedRAMP | NIST 800-171 3.1.7
22 NIST 800-53 rev4 AC-7 | ISO 27002 6.2.1 | FedRAMP | NIST 800-171 3.1.8 | PCI DSS 8.1.6 & 8.1.7 | MA201CMR17 17.04(a)(e) | CSC 16.7 | NISPOM 8-609
APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: 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:

<table>
<thead>
<tr>
<th>Classification</th>
<th>Data Classification Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SIGNIFICANT DAMAGE</strong> would occur if Restricted information were to become available to unauthorized parties either internal or external to [Company Name].</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Confidential</td>
<td>Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by [Company Name]</td>
</tr>
<tr>
<td></td>
<td>• <strong>MODERATE DAMAGE</strong> would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name].</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Internal Use</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MINIMAL or NO DAMAGE</strong> would occur if Internal Use information were to become available to unauthorized parties either internal or external to [Company Name].</td>
</tr>
<tr>
<td></td>
<td>• Impact could include damaging the company’s reputation and violating contractual requirements.</td>
</tr>
<tr>
<td>Public</td>
<td>Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NO DAMAGE</strong> would occur if Public information were to become available to parties either internal or external to [Company Name].</td>
</tr>
<tr>
<td></td>
<td>• Impact would not be damaging or a risk to business operations.</td>
</tr>
</tbody>
</table>
A-2: 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.** Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

A-3: GENERAL ASSUMPTIONS

- Any information created or received by [Company Name] employees in the performance of their jobs at the [Company Name] 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 Confidential information, the entire application is Confidential.

- Restricted, Confidential 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.

A-4: SENSITIVE PERSONAL INFORMATION (SPI)

Sensitive Personal Information (SPI) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
  - Passport number
  - Permanent resident card
- Driver License (DL)
- Financial account number
  - Payment card number (credit or debit)
  - Bank account number
- Electronic Protected Health Information (ePHI)
## Handling Controls

<table>
<thead>
<tr>
<th>Handling Controls</th>
<th>Restricted</th>
<th>Confidential</th>
<th>Internal Use</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Disclosure Agreement (NDA)</td>
<td>• NDA is required prior to access by non-[Company Name] employees.</td>
<td>• NDA is recommended prior to access by non-[Company Name] employees.</td>
<td>No NDA requirements</td>
<td>No NDA requirements</td>
</tr>
</tbody>
</table>
| Internal Network Transmission (wired & wireless) | • 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  
• Remote access should be used only when necessary and only with VPN and two-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                                                                                                           |
| 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 individuals | • Encryption is required  
• Logical access controls are required to limit unauthorized use  
• Physical access restricted to specific individuals | • 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                                                                                     |
| Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.) | • Encryption is required  
• Remote wipe must be enabled, if possible | • Encryption is required  
• Remote wipe must be enabled, if possible | • Encryption is recommended  
• Remote wipe should be enabled, if possible | No special requirements                                                                                                           |
| Email (with and without attachments)          | • Encryption is required  
• Do not forward                                                                                                                 | • Encryption is required  
• Do not forward                                                                                                                 | • Encryption is recommended                                                                                                         | No special requirements                                                                                                           |
| Physical Mail                                 | • Mark “Open by Addressee Only”  
• Use “Certified Mail” and sealed, tamper-resistant envelopes for external mailings  
• Delivery confirmation is required  
• Hand deliver internally | • Mark “Open by Addressee Only”  
• Use “Certified Mail” and sealed, tamper-resistant envelopes for external mailings  
• Delivery confirmation is required  
• Hand delivering is recommended over interoffice mail | Mail with company interoffice mail  
• US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings | No special requirements                                                                                                           |
| Printer                                       | • Verify destination printer  
• Attend printer while printing                                                                                                   | • Verify destination printer  
• Attend printer while printing                                                                                                   | • Verify destination printer  
• Retrieve printed material without delay                                                                                           | No special requirements                                                                                                           |
<table>
<thead>
<tr>
<th>Web Sites</th>
<th>Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data.</th>
<th>Posting to publicly-accessible Internet sites is prohibited.</th>
<th>Posting to publicly-accessible Internet sites is prohibited</th>
<th>No special requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td>Confirm participants on the call line</td>
<td>Confirm participants on the call line</td>
<td>No special requirements</td>
<td>No special requirements</td>
</tr>
<tr>
<td>Video / Web Conference Call</td>
<td>Pre-approve roster of attendees</td>
<td>Pre-approve roster of attendees</td>
<td>No special requirements</td>
<td>No special requirements</td>
</tr>
<tr>
<td>Fax</td>
<td>Attend receiving fax machine</td>
<td>Attend receiving fax machine</td>
<td>No special requirements</td>
<td>No special requirements</td>
</tr>
<tr>
<td>Paper, Film / Video, Microfiche</td>
<td>Return to owner for destruction</td>
<td>Shred or delete all documents or place in secure receptacle for future shredding</td>
<td>Shred or delete all documents or place in secure receptacle for future shredding</td>
<td>No special requirements</td>
</tr>
<tr>
<td>Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs / DVDs, etc.)</td>
<td>Physically destroy the hard drives and media</td>
<td>Physically destroy the hard drives and media</td>
<td>Physically destroy the hard drives and media</td>
<td>Physically destroy the hard drives and media</td>
</tr>
<tr>
<td></td>
<td>Requires use of company-approved vendor for destruction</td>
<td>Requires use of company-approved vendor for destruction</td>
<td>Requires use of company-approved vendor for destruction</td>
<td>Requires use of company-approved vendor for destruction</td>
</tr>
</tbody>
</table>
## APPENDIX B: 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.

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Sensitive Data Elements</th>
<th>Public</th>
<th>Internal Use</th>
<th>Confidential</th>
<th>Restricted</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client or Employee Personal Data</strong></td>
<td>Social Security Number (SSN)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Employer Identification Number (EIN)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Driver’s License (DL) Number</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Account Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Payment Card Number (credit or debit)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Government-Issued Identification (e.g., passport, permanent resident card, etc.)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Birth Date</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>First &amp; Last Name</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Age</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone and/or Fax Number</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Address</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethnicity</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Address</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Employee-Related Data</strong></td>
<td>Compensation &amp; Benefits Data</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medical Data</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workers Compensation Claim Data</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Education Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dependent or Beneficiary Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sales &amp; Marketing Data</strong></td>
<td>Business Plan (including marketing strategy)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Data Related to Revenue Generation</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marketing Promotions Development</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>News Releases</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Networking &amp; Infrastructure Data</strong></td>
<td>Username &amp; Password Pairs</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Public Key Infrastructure (PKI) Cryptographic Keys (public &amp; private)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardware or Software Tokens (multifactor authentication)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Configuration Settings</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regulatory Compliance Data</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal IP Addresses</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privileged Account Usernames</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Provider Account Numbers</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Strategic Financial Data</strong></td>
<td>Corporate Tax Return Information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal Billings</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Budget-Related Data</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unannounced Merger and Acquisition Information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trade Secrets (e.g., design diagrams, competitive information, etc.)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Operating Financial Data</strong></td>
<td>Electronic Payment Information (Wire Payment / ACH)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paychecks</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incentives or Bonuses (amounts or percentages)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stock Dividend Information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bank Account Information</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investment-Related Activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debt Amount Information</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC Disclosure Information</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## APPENDIX C: 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.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Record</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Records</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amendments</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Annual Reports</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Articles of Incorporation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board of Directors (elections, minutes, committees, etc.)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Bylaws</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Capital stock &amp; bond records</td>
<td></td>
<td>Permanent</td>
</tr>
<tr>
<td>Charter</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Contracts &amp; agreements</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Copyrights</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Correspondence (General)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Correspondence (Legal)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Partnership agreement</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Patents</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Servicemarks</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Stock transfers</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Trademarks</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td><strong>Financial Records</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit report (external)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Audit report (internal)</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Balance sheets</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Bank deposit slips, reconciliations &amp; statements</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Bills of lading</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Budgets</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Cash disbursement &amp; receipt record</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Checks (canceled)</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Credit memos</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Depreciation schedule</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Dividend register &amp; canceled dividend checks</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Employee expense reports</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Employee payroll records (W-2, W-4, annual earnings records, etc.)</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Financial statements (annual)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Freight bills</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>General ledger</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Internal reports (work orders, sales reports, production reports)</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Inventory lists</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Investments (sales &amp; purchases)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Profit / Loss statements</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Purchase and sales contracts</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Purchase order</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Subsidiary ledgers (accounts receivable, accounts payable, etc.)</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Tax returns</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Vendor Invoices</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Worthless securities</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td><strong>Type of Record</strong></td>
<td><strong>Retention Period</strong></td>
</tr>
<tr>
<td>Accident report / injury claim</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Category</td>
<td>Type of Record</td>
<td>Retention Period</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Personnel Records</td>
<td>Attendance Records</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Employee benefit plans</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Employment applications (not hired)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Garnishments</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>I-9 Forms</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Medical and exposure records - related to toxic substances</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Organization Charts</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>OSHA Logs</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>OSHA Training Documentation</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Patents</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Pension plan agreement</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Personnel files</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Profit sharing agreement</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Time cards and daily time reports</td>
<td>3</td>
</tr>
<tr>
<td>Insurance</td>
<td>Fire inspection reports</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Group disability records</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HIPAA-related documentation</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Insurance policies</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Safety records</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Settled insurance claims</td>
<td>7</td>
</tr>
<tr>
<td>Real Estate</td>
<td>Deeds</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Mortgages</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Plans &amp; blueprints</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Plant cost ledger</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Property appraisals</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Property register</td>
<td>Permanent</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Server audit trail history</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Workstation audit trail history</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Router audit trail history</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Firewall audit trail history</td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Visitor logs</td>
<td>1</td>
</tr>
</tbody>
</table>
APPENDIX D: 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).

D-1: 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

D-2: 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 is 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.

<table>
<thead>
<tr>
<th>Asset Categorization Matrix</th>
<th>Data Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RESTRICTED</td>
</tr>
<tr>
<td>SC-1 Mission Critical</td>
<td>Enhanced</td>
</tr>
<tr>
<td>SC-2 Business Critical</td>
<td>Enhanced</td>
</tr>
<tr>
<td>SC-3 Non-Critical</td>
<td>Enhanced</td>
</tr>
</tbody>
</table>

Figure D-1: Asset Categorization Risk Matrix

D-3: 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 cybersecurity 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.

D-4: 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 Basic Assurance level that is expanded to require more robust IT security capabilities that are commensurate with the value of the project to [Company Name].