

{Insert Company Name}

Security Policy

Awareness and Training (AT)

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

# Table of Contents

1 Introduction ..............................................................................................................................................1

2 Purpose .....................................................................................................................................................1

3 Scope .........................................................................................................................................................2

4 Roles and Responsibilities .........................................................................................................................2

5 Management Commitment ......................................................................................................................2

6 Authority ...................................................................................................................................................3

7 Compliance ...............................................................................................................................................3

8 Policy Requirements .................................................................................................................................4

8.1 Security Awareness Training; Policies and Procedures [AT-1] ..........................................................4

8.2 Security Literacy Awareness Training [AT-2, AT-2 (1,2,3)] ................................................................4

8.3 Role-Based Training [AT-3] ................................................................................................................6

8.4 Training Records [AT-4] .....................................................................................................................6

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by {Insert Company Name}’s management and in compliance with the Access Control family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s systems, facilities, and data are protected. These policies are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these policies pertain to all {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These policies apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

|  |  |  |
| --- | --- | --- |
| **Individual or Group** | **Role** | **Responsibility** |
|  | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
|  | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
|  | Information Owner | Has statutory, management, or operational authority for {Insert Company Name} information. Responsible for developing, implementing, and maintaining policies and procedures governing information generation, collection, processing, dissemination, and disposal. |
|  | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | Information Technology Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
|  | Information System Security Officer | Responsible for ensuring that the appropriate operational security posture is maintained for an information system, responsible for ensuring coordination among groups is managed and maintained for these policies/procedures. |
| System Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company Name} and its management are fully committed to protecting the confidentiality and integrity of corporate proprietary and production systems, facilities, and data as well as the availability of services in the {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company Name} Information Owner. The following applicable laws, directives, policies, regulations, and standards were used as part of the development for this policy. These include, but are not limited to:

1. E-Government Act of 2002
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. OMB Memorandum for Agency CIOs: Security Authorization of Information Systems in Cloud Computing Environments, December 2011

# Compliance

Compliance with these policies is mandatory. It is {Insert Company Name}’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these policies by using an independent audit performed by an external vendor and/or internal self-assessments to identify areas of non-compliance. Any findings identified in the audit will be remediated in accordance with the auditing team’s recommendations.

# Policy Requirements

The following personally identifiable information processing and transparency controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 Security Awareness Training Policies and Procedures [AT-1]

This document is intended to serve as the *Security Awareness and Training Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Security Awareness and Training Policy* and related controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [AT-1 (a)]

* An organizational-level Security Awareness and Training Policy that: [AT-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [AT-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [AT-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Security Awareness and Training Policy and the associated Security Awareness and Training controls [AT-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Security Awareness and Training policy and procedures. [AT-1 (b)]

{Insert Company Name} must review and update the current Security Awareness and Training: [AT-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [AT-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [AT-1 (c) (2)]

8.2 Security Literacy Awareness Training [AT-2, At-2 (1,2,3)]

{Insert Company Name} must provide security and privacy literacy training to system users including managers, senior executives, and contractors as part of initial training for new users and at least annually thereafter or when required by system changes or following any updated requirements. [(AT-2 (a) (1&2))]

{Insert Company Name} must employ techniques to increase the security and privacy awareness of system users to recognize and report potential indicators of insider threats, protecting PII, and social engineering. [(AT-2 (b)]

{Insert Company Name} must update literacy training and awareness content after an incident or at least annually. [(AT-2 (c)]

{Insert Company Name} must incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques. [(AT-2 (d)]

The security awareness training includes:

* Recognizing and reporting potential indicators of insider threats [AT-2 (2)]
* Recognizing and reporting potential and actual instances of social engineering and mining [AT-2(3)]

8.3 Role-Based Training [AT-3]

In addition to the general security awareness training required for all employees and the training required for program-specific roles, {Insert Company Name} must provide role-based security and privacy training to all personnel with roles and responsibilities in software development, systems administration, database administration, and information security. The role-based training shall be: [AT-3 (a)]

* Assigned before authorizing access to the information system or performing assigned duties and at least annually thereafter [AT-3 (a) (1)]
* Reassigned when required by system changes [AT-3 (a) (2)]
* Updated at least annually or upon a significant change to the system or role [AT-3 (b)]
* Updated to incorporate lessons learned from internal or external security incidents or breaches [AT-3 (c)]

8.4 Training Records [AT-4]

{Insert Company Name} must document and monitor individual information system security training activities including security and privacy awareness training and specific role-based security and privacy training [AT-4 (a)] and retain individual training records for at least five (5) years for High impact systems and one (1) year for all other impact systems. [AT-4 (b)]