

GovRAMP

{Insert Company Name}

Security Procedures

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

[Document Revision History 1](#_Toc153444544)

[Table of Contents 2](#_Toc153444545)

[1 Introduction 3](#_Toc153444546)

[2 Purpose 3](#_Toc153444547)

[3 Scope 3](#_Toc153444548)

[4 Roles and Responsibilities 3](#_Toc153444549)

[5 Management Commitment 4](#_Toc153444550)

[6 Authority 5](#_Toc153444551)

[7 Compliance 5](#_Toc153444552)

[8 Procedural Requirements [AT-1] 6](#_Toc153444553)

[8.1 Conducting Basic Security Awareness Training [AT-2] 6](#_Toc153444554)

[8.2 Conducting Role Based Training [AT-3] 6](#_Toc153444555)

[8.3 Retention of Training Records [AT-4] 7](#_Toc153444556)

# Introduction

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

# Purpose

The purpose of these procedures is to establish a structured approach for ensuring that all personnel are adequately trained and aware of their responsibilities in safeguarding {Insert Company Name}'s information systems. These procedures aim to promote a culture of security awareness, mitigate risks associated with human factors, and ensure compliance with the Awareness and Training Policy. Furthermore, these procedures are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these procedures 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 procedures 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 procedures 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.

# Procedural Requirements [AT-1]

The following awareness and training requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company Name} {Insert Product Name} Information System.

8.1 Conducting Basic Security Awareness Training [AT-2]

{Insert Company Name}’s security awareness training program provides instruction for all new users who access, operate, and maintain the {Insert Product Name} Information System. {Insert Company Name} utilizes and conducts training using {Insert Learning Management System tool name used for Awareness Training}.

New {Insert Product Name} Information System users are required to complete basic security awareness training as part of the onboarding process. New users are assigned the “All Users Training” which includes information security training that must be completed before access to the {Insert Product Name} Information System is granted. [AT-2 (a) (1)]

All {Insert Product Name} Information System users are required to complete basic security awareness training annually and when required by changes to the {Insert Product Name} Information System. [AT-2 (a) (2)] New annual campaigns are built at the beginning of every year, or after an incident, and automatically assigned to all employees upon the anniversary of their previous training. [AT-2(c)] {Insert Company Name} users are notified via email once they are assigned new training in {Insert tool name used for Awareness Training}.

{Insert Company Name} requires all employees with access to the {Insert Product Name} Information System to complete training for indicators of insider threats, protecting PII, and social engineering as part of general security awareness training. [AT-2 (b)] [AT-2(2)] [AT-2(3)]

If an internal or external security incident or breach occurs, lessons learned from the incident or breach are incorporated into the mandatory Security Refresher training that takes place annually. [AT-2(d)]

8.2 Conducting Role Based Training [AT-3]

The following groups receive role-based security training: [AT-3(a)]

* Developers are required to complete OWASP Top-10 training
* System Administrators are required to complete {Insert Tool Name Used} elevated privilege training
* Database Administrators are required to complete secure database administration training
* {Insert Product Name} Admin users are required to complete the {Insert Product Name} Admin training path in {Insert Tool Name Used}
* Role-Based users are required to complete the {Insert Role} training path in {Insert Tool Name Used}
* Information Security team members are required to complete the same training as all roles, including Developer, System Administrator, Database Administrator, {Insert Product Name} Admin, and {Insert Role} User

Role-based security training is required prior to a new employee accessing the {Insert Product Name} Information System, at least annually [AT-3(a) (1)], after major changes to the {Insert Product Name} Information System [AT-3(a) (2)], and when a new role is assigned to the employee. All role-based security training is provided through {Insert Tool Name Used}.

Role-based security training is updated at least annually, upon a material change to the {Insert Product Name} Information System or the role of the employee. [AT-3(b)] If an internal or external security incident or a breach occurs, training is updated with the lessons learned from the incident or breach. [AT-3(c)]

8.3 Retention of Training Records [AT-4]

The {Insert Company Name} Training Department tracks and ensures compliance for the training within {Insert Tool Name Used}. Security awareness training and role-based training records are stored in {Insert Tool Name Used} with controlled access that is limited to {Insert Tool Name Used} administrators. [AT-4(a)] Training records are retained for at least one (1) year. [AT-4(b)]