Insert Logo Here

Organization Name

Security Procedure

Awareness & Training

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published AT Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68597743)

[2 Purpose 1](#_Toc68597744)

[3 Scope 1](#_Toc68597745)

[4 Roles and Responsibilities 1](#_Toc68597746)

[5 Management Commitment 2](#_Toc68597747)

[6 Authority 3](#_Toc68597748)

[7 Compliance 3](#_Toc68597749)

[8 Procedural Requirements 4](#_Toc68597750)

[8.1 Conducting Basic Security Awareness Training 4](#_Toc68597751)

[8.2 Conducting Role Based Training 4](#_Toc68597752)

[8.3 Retention of Training Records 4](#_Toc68597753)

# Introduction

Organization Name has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by Organization Name management and in compliance with the Awareness & Training family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

This document defines the information awareness and training procedures. These procedures are in place to facilitate the implementation of the Awareness and Training Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

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

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name systems and our customer's confidential information.

| **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 Organization 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. |
|  | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
|  | 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 Manager | 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 Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

Organization 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 Organization Name system by implementing adequate security controls.

# Authority

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

1. E-Government Act of 2002/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. 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 Organization Name procedure 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 annually by an external vendor 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

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 Organization Name information systems.

## Conducting Basic Security Awareness Training

New information system users are required to complete basic security awareness training as part of the onboarding process. Organization Name utilizes {Tool/Process} as a training platform. New users are assigned Training which includes information security training that must be completed for system access.

Information system users are required to complete basic security awareness training when required by system changes and annually. Users assigned to {Roles} are required to complete the training annually, new annual campaigns are built at the beginning of every year and assigned to all members of the {Roles/Team}.

Organization Name has implemented insider threat security training in the {Tool/Process}. This training is required annually and for all new users. Completion and annual requirements are tracked by {Role}.

The {Role} is responsible for ensuring basic security awareness training for new and current information system users is available and assigned in {Tool/Process} and tracked by {Role}.

The {Role}is responsible for monitoring, tracking, and documenting basic security awareness training using {Tool/Process} Reporting to ensure compliance or view upcoming compliance deadlines. Compliance with completion of training is managed in {Tool/Process}. Automated emails are generated to report on compliance status of training.

## Conducting Role Based Training

New information system users are required to complete role-based security related training before being issued access to the information system or performing assigned duties and must complete additional training when required by system changes or annually. The {Role} is responsible for monitoring, tracking, and documenting training using the {Tool/Process} training system.

The {Role} is responsible for assigning role-based security related training to new and current information system users via Role-Based Training Procedures. Role-Based Training is assigned based on the following roles:

* {Role Type}
* {Role Type}
* {Role Type}
* {Role Type}

## Retention of Training Records

Security awareness training and role-based training records are stored in {Tool/Process} with controlled access that is limited to {Role}. Records are retained for at least three (3) years.