Insert Logo Here

Organization Name

Security Procedure

Planning

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 PL Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68607818)

[2 Purpose 1](#_Toc68607819)

[3 Scope 1](#_Toc68607820)

[4 Roles and Responsibilities 1](#_Toc68607821)

[5 Management Commitment 2](#_Toc68607822)

[6 Authority 3](#_Toc68607823)

[7 Compliance 3](#_Toc68607824)

[8 Procedural Requirements 4](#_Toc68607825)

[8.1 System Security Plan 4](#_Toc68607826)

[8.2 Rules of Behavior 4](#_Toc68607827)

[8.3 Information Security Architecture 5](#_Toc68607828)

# 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 Planning 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 security planning procedures. These procedures are in place to facilitate the implementation of the Security Planning 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 policy. 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 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 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 security planning 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.

## System Security Plan

The Organization Name System Security Plan (SSP) provides an overview of the security requirements and describes the controls in place or planned for implementation to provide a level of security appropriate for the information processed. The SSP will:

* Be consistent with the organization’s enterprise architecture
* Explicitly define the authorization boundary for the system
* Describe the operational context of the information system in terms of missions and business processes
* Provide security categorization of the information system with rationale
* Describe the operational environment of the information system and relationships with or connections to other information systems
* Provide an overview of the security requirements for the system
* Identify any relevant overlays
* Describe the security controls in place or planned for meeting those requirements, including rationale for tailoring decisions
* Be reviewed and approved by authorizing official or designated party prior to implementation

The Organization Name {Role} is responsible for the development, maintenance, and approval of the security plan which must be reviewed on an annual basis.

Copies of the Organization Name Security Plan and any updates will be distributed to the {Role}, {Role}. Organization Name will protect the security plan from unauthorized disclosure and modification by storing the SSP within the {Team/Role} secured document storage location.

The System Security Plan must be updated to address changes to the information system and environment by planning and authorizing all plan changes, updating system baseline requirements, documenting security control or system reconfigurations.

Organization Name will plan and coordinate security related activities affecting the information system with the {Team/Role}, {Team/Role}, and applicable customers before conducting such activities in order to reduce the impact on other entities.

## Rules of Behavior

All Organization Name employees must follow rules for authorized and acceptable use of Organization Name information, networks, and assets. All employees have access to the *Rules of Behavior Policy* describing personnel responsibilities and expected behavior regarding access and use of information and the information system. The *Rules of Behavior Policy* includes explicit restrictions on the use of social media, networking sites, and posting Organization Name information on public websites.

Employees must sign the *Rules of Behavior Policy* acknowledgement form inside the {Tool} indicating they have read, understand, and agree to abide by the rules of behavior, before being granted access to information and the information system.

The *Rules of Behavior Policy* must be reviewed and updated annually or when there is a major change and require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised or updated.

## Information Security Architecture

Organization Name will develop an information security architecture for the information system that describes the following:

* The overall philosophy, requirements, and approach to be taken about protecting the confidentiality, integrity, and availability of information
* How the security architecture is integrated into and supports the enterprise architecture
* Any information security assumptions about, and dependencies on, external services

Organization Name will ensure the information security architecture is reviewed by the {Team/Role} at least annually or when a significant change occurs. This review reflects updates in the enterprise architecture. Planned information security architecture changes will also be reflected in the security plan and Organization Name procurements and/or acquisitions.