Insert Logo Here

Organization Name

Security Policy

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 Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593923)

[2 Purpose 1](#_Toc68593924)

[3 Scope 1](#_Toc68593925)

[4 Roles and Responsibilities 1](#_Toc68593926)

[5 Management Commitment 2](#_Toc68593927)

[6 Authority 3](#_Toc68593928)

[7 Compliance 3](#_Toc68593929)

[8 Policy Requirements 4](#_Toc68593930)

[8.1 Security Planning Policies and Procedures 4](#_Toc68593931)

[8.2 System Security Plan 4](#_Toc68593932)

[8.3 Rules of Behavior 5](#_Toc68593933)

[8.4 Information Security Architecture 5](#_Toc68593934)

# Introduction

has developed corporate policies that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These policies are set forth by 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 4.

# Purpose

The purpose of these policies is to establish access control requirements to ensure the confidentiality, integrity, and availability of 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 employees, contractors, third parties, and others who have access to company and customer confidential information within systems and facilities.

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to 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 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

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 system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the 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 policies is mandatory. It is 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.

# Policy 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.

## Security Planning Policies and Procedures

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

The Information Owner will review and update the *Security Planning Policy* every three (3) years and the procedure(s) at least annually or any time there are significant changes in software or security. Updates must be made to keep the policy and procedure(s) in alignment with Organization Name overall business goals and risk position. Any updates, improvements, or suggestions regarding the *Security Planning Policy* and/or procedure(s) must be sent to the Information Owner.

## System Security Plan

Organization Name must develop and maintain a security plan for the information system with the following characteristics:

* Consistent with the organization’s enterprise architecture
* Explicitly defines the authorization boundary for the system
* Describes the operational context of the information system in terms of missions and business processes
* Provides the security categorization of the information system including supporting rationale
* Describes the operational environment for the information system
* Describes relationships with or connections to other information systems
* Provides an overview of the security requirements for the system
* Identifies any relevant overlays, if applicable
* Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions
* Reviewed and approved by the authorizing official or designated representative prior to plan implementation

The security plan must be distributed and/or made available to the appropriate personnel and all subsequent changes to the plan must be communicated to all authorized personnel and roles. The security plan must be reviewed at least annually, and updates must be made to reflect changes to the information environment or problems identified during plan implementation or the security control assessments. Lastly, the security plan must be protected from unauthorized disclosure and/or modification.

## Rules of Behavior

Organization Name must establish and make readily available to all information users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage

All users must sign the *Rules of Behavior Policy* acknowledging they have read, understand, and agree to abide by the rules of behavior, before being granted access to information and/or the information system. The *Rules of Behavior Policy* must be reviewed and updated at least every three (3) years. When the policy is revised or updated, employees are required to re-sign the *Rules of Behavior Policy*.

The Rules of Behavior Policy includes explicit restrictions on the use of social media, networking sites, and posting organizational information on public websites.

## Information Security Architecture

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

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

The information security architecture must be reviewed and updated at least annually to reflect updates in the enterprise architecture. Planned information security architecture changes must be reflected in the security plan, the security Concept of Operations (CONOPS), and organization procurements and/or acquisitions.