Insert Logo Here

Organization Name

Security Policy

Personnel Security

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 PS Policy | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68593907)

[2 Purpose 1](#_Toc68593908)

[3 Scope 1](#_Toc68593909)

[4 Roles and Responsibilities 1](#_Toc68593910)

[5 Management Commitment 2](#_Toc68593911)

[6 Authority 3](#_Toc68593912)

[7 Compliance 3](#_Toc68593913)

[8 Policy Requirements 4](#_Toc68593914)

[8.1 Personnel Security Policies and Procedures 4](#_Toc68593915)

[8.2 Position Categorization 4](#_Toc68593916)

[8.3 Personnel Screening 4](#_Toc68593917)

[8.4 Personnel Termination 4](#_Toc68593918)

[8.5 Personnel Transfer 5](#_Toc68593919)

[8.6 Access Agreements 5](#_Toc68593920)

[8.7 Third-Party Personnel Security 5](#_Toc68593921)

[8.8 Personnel Sanctions 5](#_Toc68593922)

# 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 personnel security 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.

## Personnel Security Policies and Procedures

This document is intended to serve as the *Personnel Security Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Personnel Security 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 *Personnel Security 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 *Personnel Security Policy* and/or procedure(s) must be sent to the Information Owner.

## Position Categorization

Organization Name must assign a risk designation to all job positions, establish screening criteria for individuals filling those positions, and review and revise position risk designation at least every three (3) years.

## Personnel Screening

Before granting assess to the information system, Organization Name must:

* Screen individuals prior to authorizing access to information, and support reinvestigation requirements as required by the customer organization
* Ensure that individuals accessing information or any system processing, storing, or transmitting information requiring special protection have valid access authorizations that are demonstrated by assigned official government duties and satisfy personnel screening criteria

## Personnel Termination

Upon termination of an individual’s employment, Organization Name must:

* Disable information access within the same day and notify appropriate personnel
* Terminate and/or revoke any authenticators and/or credentials associated with the individual
* Conduct exit interviews that include discussion of nondisclosure agreements, potential limitations on future employment, and account for information system related or company related property
* Retrieve all security related organizational information system related property
* Retain access to organizational information and information systems formerly controlled by terminated individual
* Notify Human Resources, the Information Owner, and Information Security Manager as soon as reasonably possible

## Personnel Transfer

In the event of an employee transfer, Organization Name must:

* Review and confirm the ongoing operational need for logical and physical access authorizations to information systems and/or facilities when personnel are reassigned or transferred to other positions within the organization
* Initiate transfer or reassignment actions within five (5) days of transfer
* Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer
* Notify affected clients and appropriate Organization Name personnel within twenty four (24) hours of the formal transfer action

## Access Agreements

Organization Name must develop and document access agreements for the information system and ensure that individuals requiring access to the information and information systems sign the appropriate access agreements prior to being granted access.

The access agreements must be reviewed and updated at least annually, and individuals are required to re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at least annually.

## Third-Party Personnel Security

If Organization Name uses third party personnel such as contractors, Organization Name must:

* Establish personnel security requirements including security roles and responsibilities for third party providers
* Require third party providers to comply with personnel security policies and procedures established by the organization
* Document personnel security requirements
* Require third party providers to notify the appropriate Organization Name personnel of any personnel transfers or terminations of third party personnel who possess organizational credentials and/or badges, or who have information system privileges within the same day
* Monitor provider compliance

## Personnel Sanctions

Organization Name must employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. When a formal employee sanctions process is initiated, the appropriate managers must immediately be informed of the individual who has been sanctioned and the reason for the sanction.