Insert Logo Here

Organization Name

Security Procedure

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 Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68608267)

[2 Purpose 1](#_Toc68608268)

[3 Scope 1](#_Toc68608269)

[4 Roles and Responsibilities 1](#_Toc68608270)

[5 Management Commitment 2](#_Toc68608271)

[6 Authority 3](#_Toc68608272)

[7 Compliance 3](#_Toc68608273)

[8 Procedural Requirements 4](#_Toc68608274)

[8.1 Position Categorization 4](#_Toc68608275)

[8.2 Personnel Screening 4](#_Toc68608276)

[8.3 Personnel Terminations 4](#_Toc68608277)

[8.4 Personnel Transfers 5](#_Toc68608278)

[8.5 Access Agreements 5](#_Toc68608279)

[8.6 Third Party Personnel Security 5](#_Toc68608280)

[8.7 Personnel Sanctions 6](#_Toc68608281)

# 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 Access Control 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 personnel security procedures. These procedures are in place to facilitate the implementation of the Personnel Security 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 procedures 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 personnel security requirements, mechanisms, and provisions are to be followed by all employees, management, and contractors who access and support the Organization Name information systems.

## Position Categorization

Organization Name ensures all positions are assigned a risk designation through the execution of the following actions:

* Individuals are screened according to criteria developed by the {Team/Role} based on security requirements, years with the organization, type of experience required to fill the position, and the access level authorized for the position
* A risk designation is assigned to all personnel within the information system according to the outcome of their risk assessment
* The {Team/Role} will review and update the risk designation during job announcements or at least every three (3) years.

## Personnel Screening

All individuals must be screened prior to receiving access the information system. Screening includes a criminal only background check and compliance with any additional screening correlating to the individuals position risk level. Any investigations must be initiated before appointment to high-risk position.

Access to any data specially protected for a customers or government agency will be restricted and access is only granted following an explicit approval process. A business need or justification will need to be provided and approved by the component owner, the customer information owner, and any other personnel or roles designated by the customer.

## Personnel Terminations

In the event of an employment termination, the {Team/Role} and {Team/Role} are responsible for terminating information system access upon notification by the {Team/Role} within the same day. {Team/Role} and {Team/Role} shall:

* Terminate all system accounts across all information system domains
* In the case of administrative accounts, ensure no maintenance or specialized processes are using the access credentials and verify these credentials are not the only access method to a system, prior to termination
* Ensure no local credentials are left on individual systems, in addition to terminating common Single Sign-On (SSO) credentials

The {Team/Role} will conduct exit interviews for all employees terminating employment at Organization Name. Exit interviews will be conducted with a focus on understanding security constraints, proper accountability, and non-disclosure agreements, along with business needs to review the terms of the termination, collect equipment and additional {Team/Role} related steps. Special focus will be placed on the timely execution of exit interviews for employees or contractors terminated for cause.

The {Team/Role} or designee will coordinate with the terminated employee to retrieve all security related or information system related property. The {Team/Role} will document the receipt of all returned property (hardware authentication tokens, manuals, keys, etc.) and Organization Name retains access to organizational information and information systems formerly controlled by a terminated individual.

## Personnel Transfers

The {Team/Role} reviews logical and physical access authorizations to the information system and facilities when personnel are reassigned or transferred to other positions within the organization. Transfer actions are completed within seven (7) days of a transfer and the {Team/Role} will notify relevant parties within one (1) day of completion. Based on the review, the {Team/Role} will:

* Ensure old access keys and/or tokens are returned, and new items are issued to support new responsibilities
* Ensure previous system accounts are terminated and new accounts with appropriate access are established
* Ensure information system access authorizations are changed to support new responsibilities

## Access Agreements

New Organization Name employees are required to review and sign access agreements prior to receiving access to the Organization Name information system. The access agreements consist of the following documents:

* Rules of Behavior (ROB)
* Acceptable Use Policy (AUP)
* Non-Disclosure Agreement (NDA)

ROB and AUP signatures are retained within the Organization Name {Tool} and the {Team/Role} retains NDA signatures.

The {Team/Role} must review the ROB and AUP at least annually and adjust the content of the agreements, as necessary. If changes are made to the agreements, employees are required to review the updated access agreements and re-sign to acknowledge and accept the changes to the agreement.

## Third Party Personnel Security

The {Team/Role} is responsible for establishing and documenting security roles and responsibilities for third party providers. These roles may be similar but not identical to the roles and responsibilities of employees. Third party personnel must abide by the same personnel security requirements as employees and violations of security requirements may result in termination of access or contract.

Third party personnel are monitored by the {Team/Role} for compliance. Third party personnel are also required to sign the Organization Name NDA, ROB, and AUP as well as completing any training relevant to their position. Organization Name also requires third party providers to notify the Organization Name {Team/Role} and {Team/Role} of any personnel transfers or terminations of third-party personnel who possess Organization Name credentials and/or badges, or who have system access within the same day.

## Personnel Sanctions

In the event of a violation, the {Team/Role} will manage employee sanctions or disciplinary actions with the appropriate parties.