

GovRAMP

{Insert CompanY Name}

Security Procedures

Personnel Security [PS]

**Version:**

{N.N}

**Date:**

{Insert Modified Date}

# Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Any item that needs to be updated within this document can be found with { } around each item and in (RED) Font. [Delete this for final product submission]

Table of Contents[Document Revision History 1](#_Toc196467141)

[Table of Contents 2](#_Toc196467142)

[1 Introduction 4](#_Toc196467143)

[2 Purpose 4](#_Toc196467144)

[3 Scope 4](#_Toc196467145)

[4 Roles and Responsibilities 4](#_Toc196467146)

[5 Management Commitment 5](#_Toc196467147)

[6 Authority 6](#_Toc196467148)

[7 Compliance 6](#_Toc196467149)

[8 Procedural Requirements [PS-1] 7](#_Toc196467150)

[8.1 Position Categorization [PS-2] 7](#_Toc196467151)

[8.2 Personnel Screening [PS-3] 7](#_Toc196467152)

[8.3 Personnel Terminations [PS-4] 8](#_Toc196467153)

[8.4 Personnel Transfers [PS-5] 8](#_Toc196467154)

[8.5 Access Agreements [PS-6] 9](#_Toc196467155)

[8.6 Third-Party Personnel Security [PS-7] 9](#_Toc196467156)

[8.7 Personnel Sanctions [PS-8] 10](#_Toc196467157)

[8.8 Position Descriptions [PS-9] 10](#_Toc196467158)

# Introduction

{Insert Company Name} has developed corporate procedures that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by {Insert Company Name}’s management and in compliance with the Personnel Security family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these procedures is to establish processes for managing personnel security within {Insert Company Name}. These procedures ensure that all personnel with access to organizational systems meet security requirements and comply with the Personnel Security Policy and applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these procedures pertain to all {Insert Company Name} employees, contractors, third parties, and others who have access to company and customer confidential information within {Insert Company Name} systems and facilities.

# Roles and Responsibilities

These procedures apply to all {Insert Company Name} employees, contractors, business partners, third parties, and others who need or have access to {Insert Company Name}’s systems and our customer's confidential information. {Insert Company Personnel below and delete this for final product}

| **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 {Insert Company 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. |
|  | Chief Information Security Officer | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
|  | 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 Director | 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 Admin Team | System Administrator | Responsible for conducting information system security Administration activities. |
| Varies | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures. |
| Varies | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

{Insert Company 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 {Insert Company Name} Information System by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the {Insert Company 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
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. The Privacy Act of 1974
4. Clinger-Cohen Act of 1996
5. OMB Circulars and Memoranda
6. Federal Information Processing Standards (FIPS)
7. NIST Special Publications
8. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
9. 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 {Insert Company Name}’s policy that production systems meet or exceed the requirements outlined in this document. The Information Owner will periodically assess compliance with these procedures by using an independent audit performed by an external vendor and/or internal self-assessments 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 [PS-1]

The following personnel security requirements, mechanisms, and provisions are to be followed by all employees, management, and contractors who access and support the {Insert Company Name} information systems.

* 1. Position Categorization [PS-2]

{Insert Company Name} ensures all positions are assigned a risk designation through the execution of the following actions: [PS-2 (a)]

* Individuals are screened according to criteria developed by the {Insert Human Resources Team Name} Team based on security requirements, years with the organization, type of experience required to fill the position, and the access level authorized for the position. The {Insert Personnel Screening Service Name} screening service is used to conduct a background check that consists of (but is not limited to): [PS-2 (b)]

**{Adjust list, below, to match organizational and StateRAMP requirements}**

* + {Criminal felony & misdemeanor check}
  + {Federal criminal check}
  + {Sex offender check}
  + {Credit check (anyone filling a financial role)}
  + {SSN Trace}
  + {SSN Validation}
  + {National Criminal Search}
  + {Motor Vehicle Report (MVR) (on a subset of employees)}
* A risk designation is assigned to all personnel within the information system according to the outcome of their risk assessment
* The {Insert Human Resources Team Name} Team will review and update the risk designation during job announcements or at least every three (3) years. [PS-2 (c)]
  1. Personnel Screening [PS-3]

All individuals must be screened prior to receiving access to the {Insert Product Name} Information System. [PS-3 (a)] Screening includes a criminal only background check and compliance with any additional screening correlating to the individual’s position risk level, which is at the discretion of the government agency. 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. [PS-3 (3)]

If national security clearances are required for a customer agency, the customer agency must verify (in accordance with the following criteria) and {Insert Company Name} must get {Insert Company Name}’s individuals rescreened in accordance with the following criteria: [PS-3 (b)]

* For top secret clearances, a reinvestigation is required during the fifth (5th) year
* For secret clearances, a reinvestigation is required during the tenth (10th) year
* For confidential clearances, a reinvestigation is required during the fifteenth (15th) year
  1. Personnel Terminations [PS-4]

In the event of an employment termination, the {Insert Information Technology Team Name} and {Insert Information Security Team Name} are responsible for terminating information system access upon notification by the {Insert Human Resources Team Name} Team within four (4) hours. [PS-4 (a)] Information Technology and Information Security shall:

* Terminate all system accounts across all information system domains associated with the terminated individual [PS-4 (b)]
* 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 {Insert Human Resources Team Name} Team will conduct exit interviews for all employees terminating their employment at {Insert Company 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 {Insert Human Resources Team Name} related steps. [A special focus will be placed on the timely execution of exit interviews for employees or contractors terminated for cause. [PS-4 (c)]

The {Insert Human Resources Team Name} Team or designee will coordinate with the terminated employee to retrieve all security related or information system related property. [PS-4 (d)] The {Insert Information Technology Team Name} will document the receipt of all returned property (hardware authentication tokens, manuals, keys, etc.). {Insert Company Name} retains access to organizational information and information systems formerly controlled by a terminated individual. [PS-4 (e)]

* 1. Personnel Transfers [PS-5]

The {Insert Information Technology Team Name} reviews logical and physical access authorizations to the {Insert Product Name} Information System and facilities when personnel are reassigned or transferred to other positions within the organization. [PS-5 (a)] Transfer actions are completed within seven one (1) day of a transfer [PS-5 (b)] and the {Insert Human Resources Team Name} Team will notify relevant parties within one (1) day of completion. [PS-5 (d)] Based on the review, the {Insert Information Technology Team Name} will: [PS-5 (c)]

* 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

The {Insert Human Resources Team Name} Team manages position designation, description, and includes rights and roles assigned to positions. Changes to permissions for a specific position are brought before the {Insert name of Change Management Board}, voted on, and changed. Updated role assignments are then provided to the {Insert Human Resources Team Name} Team with a description of the privileges changed to allow for updated risk designations, and the {Insert Human Resources Team Name} Team creates a ticket in the {Insert Company Name} {Insert name of helpdesk tracking system} on either the day of or before the transfer action.

* 1. Access Agreements [PS-6]

New {Insert Company Name} employees are required to review and sign {Insert Company Name} developed access agreements prior to receiving access to the {Insert Company Name} {Insert Product Name} Information System. [PS-6 (a)] [PS-6 (c) (1)] 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 {Insert Company Name} Learning Management System (LMS), and the {Insert Human Resources Team Name} Team retains NDA signatures. The ROB and the AUP are the formal access agreement for the {Insert Product Name} Information System.

The {Insert Information Security Team Name}, {Insert Human Resources Team Name} Team, and {Insert Legal Team Name} must review the RoB and AUP at least annually and adjust the content of the agreements as necessary. [PS-6 (b)] 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. [PS-6 (c) (2)]

* 1. Third-Party Personnel Security [PS-7]

The {Insert Human Resources Team Name} Team and the {Insert Information Security Team Name} are responsible for establishing and documenting security roles and responsibilities for third-party providers. [PS-7 (a)] 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. [PS-7 (b)] The contract between {Insert Company Name} and the third-party provider documents the security requirements based upon the type of work performed by the third-party provider. [PS-7 (c)]

Third-party providers are required to notify {Insert Company Name} of any Personnel transfers or terminations of third-party personnel who possess {Insert Company Name} credentials and/or badges, or who have system access. The notifications are done on the same day or within 24 hours if unable to coordinate account deactivation with the time of transfer or termination. Upon notification by the third-party, the {Insert Company Name} {Insert Information Technology Team Name} and {Insert Badge Access Control Team Name} verifies that all two-factor authenticators, accounts, and any other access credentials are revoked and/or terminated by the appropriate {Insert Information Technology Team Name} members. At this time, all the individuals’s accounts are closed, access to the system is terminated, and all authenticators and other system support resources are returned to the company. [PS-7 (d)]

{Insert Company Name} has implemented the required security policies for third-party providers. {Insert Company Name} ensures that third party providers comply with personnel security policies and procedures established by {Insert Company Name}. [PS-7 (e)] Third-party personnel are also required to sign the {Insert Company Name} NDA, ROB, and AUP as well as completing any training relevant to their position.

* 1. Personnel Sanctions [PS-8]

In the event of a violation, the {Insert Human Resources Team Name} Team will manage employee sanctions or disciplinary actions with the appropriate parties. [PS-8 (a)]

Sanctions range from verbal warning and/or counseling session (performance improvement plan), to a formal written warning or termination depending on the nature of the infraction. The {Insert Company Name} {Insert Human Resources Team Name} Team is responsible for managing any personnel sanctions with the appropriate parties.

Once a personnel sanction is imposed, the {Insert Human Resources Team Name} Team notifies the appropriate parties, which may include executive level managers, {Insert Legal Team Name}, the {Insert Information Technology Team Name}, the {Insert Information Security Team Name}, the ISSO and/or similar role within the organization as deemed appropriate within twenty-four (24) hours. [PS-8 (b)]

NOTE: Sanctions may range from verbal warning and/or counseling session (performance improvement plan), a formal written warning, or up to termination depending on the nature of the infraction.

* 1. Position Descriptions [PS-9]

{Insert Company Name} incorporates security and privacy roles and responsibilities into organizational position descriptions. [PS-9]