

GovRAMP

{Insert Company Name}

Security Policy

Personnel Security

**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](#_Toc196402157)

[Table of Contents 2](#_Toc196402158)

[1 Introduction 3](#_Toc196402159)

[2 Purpose 3](#_Toc196402160)

[3 Scope 3](#_Toc196402161)

[4 Roles and Responsibilities 3](#_Toc196402162)

[5 Management Commitment 4](#_Toc196402163)

[6 Authority 5](#_Toc196402164)

[7 Compliance 5](#_Toc196402165)

[8 Policy Requirements 5](#_Toc196402166)

[8.1 Personnel Security Policies and Procedures [PS-1] 5](#_Toc196402167)

[8.2 Position Risk Designation [PS-2] 6](#_Toc196402168)

[8.3 Personnel Screening [PS-3] 6](#_Toc196402169)

[8.4 Personnel Termination [PS-4, {PS-4 (2) High Only] 6](#_Toc196402170)

[8.5 Personnel Transfer [PS-5] 7](#_Toc196402171)

[8.6 Access Agreements [PS-6] 7](#_Toc196402172)

[8.7 External Personnel Security [PS-7] 7](#_Toc196402173)

[8.8 Personnel Sanctions [PS-8] 8](#_Toc196402174)

[8.9 Position Descriptions [PS-9] 8](#_Toc196402175)

# Introduction

{Insert Company Name} has developed corporate policies that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These policies 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 policies is to establish Personnel Security requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s 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 {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 policies 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 policies 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 policies 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.

# Policy Requirements

The following Personnel Security controls requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support information systems owned and operated by {Insert Company Name}, including its subsidiaries and affiliates, collectively referred to as {Insert Company/Product Name}.

8.1 Personnel Security Policies and Procedures [PS-1]

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 controls have been developed, documented, and disseminated to all applicable personnel.

{Insert Company Name} must develop, document, and disseminate to all personnel including the chief privacy officer, ISSO, and/or similar roles or their designees: [PS-1 (a)]

* An organizational-level Personnel Security Policy that: [PS-1 (a) (1)]
  + Addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance [PS-1 (a) (1) (a)]
  + Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines [PS-1 (a) (1) (b)]
* Procedures to facilitate the implementation of Personnel Security Policy and the associated Personnel Security controls [PS-1 (a) (2)]

{Insert Company Name} must designate a Chief Information Security Officer (CISO) to manage the development, documentation, and dissemination of the Personnel Security policy and procedures. [PS-1 (b)]

{Insert Company Name} must review and update the current Personnel Security: [PS-1 (c)]

* Policies at least annually, following a significant change, and/or any compromising event [PS-1 (c) (1)]
* Procedures at least annually, following a significant change, and/or any compromising event [PS-1 (c) (2)]

8.2 Position Risk Designation [PS-2]

{Insert Company 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 annually for high impact systems and every three (3) years for all others.

8.3 Personnel Screening [PS-3]

Before granting access to a {Insert Company Name} Information System, {Insert Company Name} must:

* Screen individuals prior to authorizing access to the system [PS-1 (a)]
* For systems that store or process federal information: [PS-1 (b)]
  + {Insert Company Name} must support reinvestigation, if applicable, for national security clearances.

Reinvestigation is required in the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance.

For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year.

No reinvestigation is required for other moderate risk positions or any low-risk positions.

* Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection have satisfied personnel screening criteria by having a valid access authorization that are demonstrated by assigned official duties as required by specific information. [PS-3 (3) (a), (b)]

8.4 Personnel Termination [PS-4, {PS-4 (2) High Only]

Upon termination of an individual’s employment, {Insert Company Name} must:

* Disable information access within one (1) hour for high impact systems and four (4) hours for all others and notify appropriate personnel [PS-4 (a)]
* Terminate and/or revoke any authenticators and/or credentials associated with the individual [PS-4 (b)]
* Conduct exit interviews that include discussion of nondisclosure agreements, potential limitations on future employment, and account for information system related or company related property [PS-4 (c)] Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment.
* Retrieve all security related organizational information system related property [PS-4 (d)]
* Retain access to organizational information and information systems formerly controlled by terminated individual [PS-4 (e)]

**For high impact systems only:**

* Automate the notification to Human Resources, the Information System Owner, manager of the terminated employee, and IT Team when system access has been terminated. [PS-4 (2)]

8.5 Personnel Transfer [PS-5]

In the event of an employee transfer, {Insert Company 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 [PS-5 (a)]
* Initiate transfer or reassignment actions within twenty-four (24) hours following the formal transfer action [PS-5 (b)]

**NOTE**: Personnel may need to retain access to systems while training their replacement.

* Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer [PS-5 (c)]
* Notify affected clients and appropriate {Insert Company Name} personnel, including access control personnel responsible for the system, within twenty-four (24) hours of the formal transfer action [PS-4 (d)]

8.6 Access Agreements [PS-6]

{Insert Company Name} must develop and document access agreements for Information Systems and ensure that individuals requiring access to the information and information system sign the appropriate access agreements prior to being granted access. [PS-6 (a)]

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 at least annually or any time there is a material change to the user’s level of access. [PS-6 (b) (c)]

8.7 External Personnel Security [PS-7]

When {Insert Company Name} uses third-party personnel such as contractors, {Insert Company Name} must:

* Establish personnel security requirements including security roles and responsibilities for third-party providers [PS-7 (a)]
* Require third-party providers to comply with personnel security policies and procedures established by the organization [PS-7 (b)]
* Document personnel security requirements [PS-7 (c)]
* Require third-party providers to notify the appropriate {Insert Company Name} personnel of any terminations within the same day or (immediately for high impact systems) of third-party personnel who possess {Insert Company Name} credentials and/or badges. And require third-party providers to notify the appropriate {Insert Company Name} personnel of any personnel who have been transferred within twenty-four (24) hours [PS-7 (d)]
* Monitor provider compliance with personnel security requirements [PS-7 (e)]

8.8 Personnel Sanctions [PS-8]

{Insert Company Name} must employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. [PS-8 (a)]

{Insert Company Name} must notify within twenty-four (24) hours the employee’s immediate manager, the ISSO (and/or similar role within the organization) when a formal employee sanctions process is initiated, identifying the individual who has been sanctioned. [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.

8.9 Position Descriptions [PS-9]

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