

GovRAMP

{Insert Company Name}

Security Policy

Security Planning

**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](#_Toc196401807)

[Table of Contents 2](#_Toc196401808)

[1 Introduction 3](#_Toc196401809)

[2 Purpose 3](#_Toc196401810)

[3 Scope 3](#_Toc196401811)

[4 Roles and Responsibilities 3](#_Toc196401812)

[5 Management Commitment 4](#_Toc196401813)

[6 Authority 5](#_Toc196401814)

[7 Compliance 5](#_Toc196401815)

[8 Policy Requirements 5](#_Toc196401816)

[8.1 Security Planning Policies and Procedures [PL-1] 5](#_Toc196401817)

[8.2 System Security and Privacy Plans [PL-2] 6](#_Toc196401818)

[8.3 Rules of Behavior [PL-4, PL-4 (1)] 7](#_Toc196401819)

[8.4 Security and Privacy Architectures [PL-8] 7](#_Toc196401820)

[8.5 Baseline Selection [PL-10] 7](#_Toc196401821)

[8.6 Baseline Tailoring [PL-11] 8](#_Toc196401822)

# 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 Planning 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 Panning r 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 Planning 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 Security Planning Policies and Procedures [PL-1]

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 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: [PL-1 (a)]

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

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

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

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

8.2 System Security and Privacy Plans [PL-2]

{Insert Company Name} must:

* Develop and maintain a security plan for its Information Systems with the following characteristics:
  + Is consistent with the organization’s enterprise architecture [PL-2 (a) (1)]
  + Explicitly defines the authorization boundary for the information system [PL-2 (a) (2)]
  + Describes the operational context of the information system in terms of missions and business processes [PL-2 (a) (3)]
  + Identify the individuals that fulfill system roles and responsibilities to include chief privacy and ISSO and/or similar role or designees [PL-2 (a) (4)]
  + Identify the information types processed, stored, and transmitted by the system [PL-2 (a) (5)]
  + Provides the security categorization of the information system including supporting rationale [PL-2 (a) (6)]
  + Describe any specific threats to the system that are of concern to the organization [PL-2 (a) (7)]
  + Provide the results of a privacy risk assessment for systems processing personally identifiable information [PL-2 (a) (8)]
  + Describes the operational environment for the information system and any dependencies on or connections to other systems or system components [PL-2 (a) (9)]
  + Provides an overview of the security and privacy requirements for the information system [PL-2 (a) (10)]
  + Identifies any relevant control baselines or overlays, if applicable [PL-2 (a) (11)]
  + Describes the security controls in place or planned for meeting the security and privacy requirements, including a rationale for the tailoring and supplementation decisions [PL-2 (a) (12)]
  + Include risk determinations for security and privacy architecture and design decisions [PL-2 (a) (13)]
  + Include security-related and privacy-related activities affecting the system that require planning and coordination with the {Insert Information Technology Team Name} Team [PL-2 (a) (14)]
  + Reviewed and approved by the Authorizing Official (AO) or designated representative prior to plan implementation [PL-2 (a) (15)]
* Distribute copies of the plans and communicate subsequent changes to the plans to all personnel who have been designated including the chief privacy and ISSO and/or similar role [PL-2 (b)]
* Review the plans at least annually or when significant changes occur [PL-2 (c)]
* Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments [PL-2 (d)]
* Protect the plans from unauthorized disclosure and modification [PL-2 (e)]

8.3 Rules of Behavior [PL-4, PL-4 (1)]

{Insert Company Name} must establish and make readily available to all {Insert Company Name} Information System users, the rules that describe their responsibilities and expected behavior regarding information and the information system usage, security, and privacy. [PL-4 (a)]

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. [PL-2 (4) (b)] The *Rules of Behavior Policy* must be reviewed and updated at least annually. [PL-4 (c)] The employees must review and re-sign annually the *Rules of Behavior* or when the document is revised and/or updated. [PL-4 (d)]

The Rules of Behavior Policy must include explicit restrictions on:

* The use of social media, social networking sites, and external sites/applications [PL-4 (1) (a)]
* The posting organizational information on public websites [PL-4 (1) (b)]
* The use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications. [PL-4 (1) (c)]

8.4 Security and Privacy Architectures [PL-8]

{Insert Company Name} must develop an information security architecture for information that describes the following:

* Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information [PL-8 (a) (1)]
* Describe the requirements and approaches to be taken for processing PII to minimize privacy risk to individuals [PL-8 (a) (2)]
* Describe how the information security architecture is integrated into and supports the enterprise architecture [PL-8 (a) (3)]
* Any information security assumptions about, and dependencies on, external system and services [PL-8 (a) (4)]

The information security architecture must be reviewed and updated at least annually or when a significant change occurs to reflect updates in the enterprise architecture. [PL-8 (b)] Planned information security architecture changes must be reflected in the security plan, the security Concept of Operations (CONOPS), criticality analysis, organization procurements and/or acquisitions. [PL-8 (c)]

8.5 Baseline Selection [PL-10]

Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals’s privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints.

{Insert Company Name} must select a control baseline by using FIPS 199 worksheet to determine a system’s impact level and the NIST SP 800-53B to determine the baseline controls from a pre-defined sets of controls specifically to address the protection required for individual information systems based on the designated impact level. [PL-10]

8.6 Baseline Tailoring [PL-11]

The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation.

{Insert Company Name} understands that not all controls in current NIST SP 800-53 series can be implemented, necessitating tailoring. {Insert Company Name} may tailor the selected control baseline by applying specified tailoring actions. [PL-11] Tailoring guidance is provided in SP 800-53B.