

GovRAMP

{Insert CompanY Name}

Security Procedures

Security Planning [PL]

**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](#_Toc196481867)

[Table of Contents 2](#_Toc196481868)

[1 Introduction 3](#_Toc196481869)

[2 Purpose 3](#_Toc196481870)

[3 Scope 3](#_Toc196481871)

[4 Roles and Responsibilities 3](#_Toc196481872)

[5 Management Commitment 4](#_Toc196481873)

[6 Authority 5](#_Toc196481874)

[7 Compliance 5](#_Toc196481875)

[8 Procedural Requirements [PL-1] 6](#_Toc196481876)

[8.1 System Security Plan [PL-2, PL-2 (3)] 6](#_Toc196481877)

[8.2 Rules of Behavior [PL-4, PL-4 (1)] 7](#_Toc196481878)

[8.3 Information Security and Privacy Architecture [PL-8] 7](#_Toc196481879)

[8.4 Baseline Selection [PL-10] 7](#_Toc196481880)

[8.5 Baseline Tailoring [PL-11] 8](#_Toc196481881)

# 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 Security 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 procedures is to outline the processes for developing, implementing, and maintaining security plans for {Insert Company Name}'s information systems. These procedures ensure the protection of organizational data, support compliance with the Security Planning 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 [PL-1]

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

# System Security Plan [PL-2, PL-2 (3)]

The {Insert Company Name} {Insert Product Name} System Security Plan (SSP) provides an overview of the security requirements and describes the controls in place or planned for implementation to provide a level of security appropriate for the information processed. The SSP: [PL-2 (a)]

* Is consistent with the organization’s enterprise architecture [PL-2 (a) (1)]
* Explicitly defines the authorization boundary for the system [PL-2 (a) (2)]
* Describes the operational context of the information system in terms of missions and business processes [PL-2 (a) (3)]
* Identifies the individuals that fulfill system roles and responsibilities to include chief privacy and ISSO and/or similar role or designees [PL-2 (a) (4)]
* Identifies the information types processed, stored, and transmitted by the system [PL-2 (a) (5)]
* Provides security categorization of the information system with rationale [PL-2 (a) (6)]
* Describes any specific threats to the system that are of concern to the organization [PL-2 (a) (7)]
* Provides the results of a privacy risk assessment for systems processing personally identifiable information [PL-2 (a) (8)]
* Describes the operational environment of the information system and relationships with or connections to other information systems [PL-2 (a) (9)]
* Provides an overview of the security requirements for the system [PL-2 (a) (10)]
* Identifies any relevant overlays, if applicable [PL-2 (a) (11)]
* Describes the security controls in place or planned for meeting those requirements, including rationale for tailoring decisions [PL-2 (a) (12)]
* Includes risk determinations for security and privacy architecture and design decisions [PL-2 (a) (13)]
* Is reviewed and approved by authorizing official or designated party prior to implementation [PL-2 (a) (15)]

The {Insert Company Name} Information Security Manager is responsible for the development, maintenance, and approval of the security plan which must be reviewed on an annual basis. [PL-2 (c)]

Copies of the {Insert Company Name} Security Plan and any updates are distributed to the Information Security Team, Information Technology Team, and Development Team. [PL-2 (b)]

{Insert Company Name} protects the security plan from unauthorized disclosure and modification by storing the SSP within the Information Security Team’s secured {Insert Documentation Repository Name}. [PL-2 (e)]

The System Security Plan must be updated to address changes to the {Insert Product Name} Information System and environment by planning and authorizing all plan changes, updating system baseline requirements, documenting security control or system reconfigurations. [PL-2 (d)] Only those with {Insert Product Name} roles are authorized access to the system documentation.

{Insert Company Name} will plan and coordinate security and privacy related activities affecting the {Insert Product Name} Information System with the Information Technology Team, the Development Team, {Insert Vendor(s) Name}, and applicable customers before conducting such activities in order to reduce the impact on other entities. [PL-2 (a) (14)]

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

All {Insert Company Name} employees must follow rules for authorized and acceptable use of {Insert Company Name}’s information, networks, and assets. All employees have access to the *Rules of Behavior Policy* describing personnel responsibilities and expected behavior regarding access and use of information and the information system. [PL-4 (a)] The *Rules of Behavior Policy* includes explicit restrictions on:

* The use of social media and networking sites [PL-4 (1) (a)]
* Posting {Insert Company Name} information on public websites [PL-4 (1) (b)]
* The use of organization provided identifiers and authenticators for creating accounts on external sites and applications [PL-4 (1) (c)]

Employees must sign the *Rules of Behavior Policy* acknowledgement form inside the {Insert Documentation Repository Name}, indicating they have read, understand, and agree to abide by the rules of behavior, before being granted access to information and the information system. [PL-4 (b)]

The *Rules of Behavior Policy* must be reviewed and updated annually or when there is a major change, [PL-4 (c)] and require individuals who have signed a previous version of the rules of behavior to read and re-sign annually and when there has been a major revision or update to the rules of behavior.

# Information Security and Privacy Architecture [PL-8]

{Insert Company Name} has developed an information security architecture for the {Insert Product Name} Information System that describes the following: [PL-8 (a)]

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

{Insert Company Name} ensures the information security architecture is reviewed by the Information Security Manager at least annually and/or when a significant change occurs. [PL-8 (b)] This review reflects updates to the {Insert Product Name} Information System. Planned information security and privacy architecture changes will also be reflected in the System Security Plan, along with {Insert Company Name} procurements and/or acquisitions and other security-related documentation based on changes identified in a {Insert Documentation Repository Name} request. [PL-8 (c)]

# Baseline Selection [PL-10]

{Insert Company Name} adheres to the GovRAMP Moderate baseline for the {Insert Product Name} Information System.

# Baseline Tailoring [PL-11]

In the event that {Insert Company Name} would need to tailor the GovRAMP Moderate baseline, tailoring decisions would be discussed and approved by the Information Security Manager and the customer Authorizing Official or GovRAMP Board Members when appropriate. These tailoring decisions would be documented in the respective procedure documents.