

GovrAMP

{Insert Company Name}

Security Policy

Security Assessment and Authorization

**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](#_Toc196391875)

[Table of Contents 2](#_Toc196391876)

[1 Introduction 3](#_Toc196391877)

[2 Purpose 3](#_Toc196391878)

[3 Scope 3](#_Toc196391879)

[4 Roles and Responsibilities 3](#_Toc196391880)

[5 Management Commitment 4](#_Toc196391881)

[6 Authority 5](#_Toc196391882)

[7 Compliance 5](#_Toc196391883)

[8 Policy Requirements 5](#_Toc196391884)

[8.1 Security Assessment and Authorization Policies and Procedures [CA-1] 5](#_Toc196391886)

[8.2 Control Assessments [CA-2, CA-2 (1,3), {CA-2 (2) High Only}] 6](#_Toc196391887)

[8.3 Leveraging Results from External Organzations [CA-2 (3)] 7](#_Toc196391888)

[8.4 Information Exchange [CA-3, {CA-3 (6) High Only] 7](#_Toc196391889)

[8.5 Plan of Action and Milestones [CA-5] 7](#_Toc196391890)

[8.6 Authorization [CA-6] 7](#_Toc196391891)

[8.7 Continuous Monitoring [CA-7, CA-7 (1,4)] 8](#_Toc196391892)

[8.8 Penetration Testing [CA-8, CA-8 (1,2)] 8](#_Toc196391893)

[8.9 Internal System Connections [CA-9] 8](#_Toc196391894)

# 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 Security Assessment and Authorization 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 Security Assessment and Authorization 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 Security Assessment and Authorization 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 Assessment and Authorization Policies and Procedures [CA-1]

This document is intended to serve as the *Security Assessment and Authorization Policy* and is made available to all applicable personnel. The associated procedure(s) to facilitate the implementation of the *Security Assessment and Authorization 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: [CA-1 (a)]

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

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

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

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

8.2 Control Assessments [CA-2, CA-2 (1,3), {CA-2 (2) High Only}]

{Insert Company Name} must select an appropriate assessor or assessment team for the type of assessment to be conducted [CA-2 (a)] and develop a security assessment plan that describes the scope of the assessment to include [CA-2 (b)]:

* Controls and control enhancements under assessment
* Assessment procedures to be used to determine security control effectiveness
* Assessment environment, assessment team, and assessment roles and responsibilities

For StateRAMP assessments, {Insert Company Name} must employ an independent assessors or assessment team to conduct control assessments at least annually. The assessment must be conducted by an accredited American Association for Laboratory Accreditation (A2LA) Third-Party Assessment Organization (3PAO). [CA-2 (1)]

{Insert Company Name} must ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment. [CA-2 (c)]

The controls in the system and its environment of operation must be assessed at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements. [CA-2 (d)]

The assessor or assessment team must produce a control assessment report that document the results of the assessment [CA-2 (e)] and {Insert Company Name} must provide the results of the control assessment to Information Security Team, the StateRAMP PMO, and the customer Authorizing Official (AO) or StateRAMP Approvals Committee (SAC). [CA-2 (f)]

**For high impact systems only:**

As part of the annual security control assessments, {Insert Company Name} may conduct additional announced or unannounced in-depth monitoring, security instrumentation, automated security test cases, vulnerability scanning, insider threat assessments, malicious user testing, performance and load testing, data leakage, or data loss assessment. [CA-2 (2)]

8.3 Leveraging Results from External Organzations [CA-2 (3)]

{Insert Company Name} and its assessors may leverage the results of control assessments performed by any A2LA Accredited 3PAO when the assessment meets the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. [CA-2 (3)]

8.4 Information Exchange [CA-3, {CA-3 (6) High Only]

{Insert Company Name} must authorize and manage connections from internal information systems to systems outside of the authorization boundary by using one or more of the following: [CA-3 (a)]

* Interconnection Security Agreements (ISA)
* Information Exchange Security Agreements (IESA)
* Memoranda of Understanding or Agreement (MOU/MOA)
* Service Level Agreements (SLA)
* User Agreements or Contract
* Nondisclosure Agreement (NDA)

The parties must document as part of each interconnection, the interface characteristics, security and privacy requirements, controls and responsibilities for each system, and the impact of the information communicated. [CA-3 (b)] Refer to Access Control document section 8.16 External Information Systems [AC-20] and section 8.17 Information Sharing [AC-21] for minimum requirements.

The Interconnection Security Agreements must be reviewed and updated at least annually and input from the Authorizing Official (AO) or StateRAMP Approvals Committee (SAC).

**For high impact systems only:**

{Insert Company Name} must verify that individuals or systems transferring data between interconnected systems have the requisite authorizations, (written permissions or privileges) at the proper impact level prior to accepting such data. [CA-3 (6)]

8.5 Plan of Action and Milestones [CA-5]

A Plan of Action and Milestones (POA&M) must be developed to document the planned remediation actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system during continuous monitoring activities.

The existing POA&M must be updated at least monthly based on the findings from control assessments, impact analyses, independent audits or reviews, and continuous monitoring activities. POA&Ms must be delivered to all agency customer Authorizing Officials and the StateRAMP PMO at least monthly.

8.6 Authorization [CA-6]

{Insert Company Name} must assign a senior-level executive or manager to the role of the Authorizing Official (AO) for each system and for common controls available for inheritance by organizational systems. [CA-6 (a, b)]

Before commencing operations, {Insert Company Name} must ensure the AO:

* Authorizes the system to operate [CA-6 (c) (2)]
* Accepts the use common controls available for inheritance by the system [CA-6 (c) (1)]
* Authorizes the use of those controls for inheritance by organizational systems [CA-6 (d)]

Authorizations must be update annually, in accordance with OMB-130 requirements, and when a significant change occurs as defined in NIST SP800-37 r2, Appendix F and/or according to StateRAMP Significant Change to Policies and Procedures. [CA-6 (e)]

8.7 Continuous Monitoring [CA-7, CA-7 (1,4)]

{Insert Company Name} must work in conjunction with sponsoring agency customers to establish a continuous monitoring strategy and implement a continuous monitoring program that includes: [CA-7]

* Establishment of metrics identified by the *StateRAMP Continuous Monitoring Strategy Guide*, as appropriate [CA-7 (a)]
* Establish at least monthly monitoring and at least annual assessment of control effectiveness [CA-7 (b)]
* Ongoing security control assessments in accordance with the information continuous monitoring strategy [CA-7 (c)]
* Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy [CA-7 (d)]
* Correlation and analysis of security-related information generated by assessments and monitoring [CA-7 (e)]
* Response actions to address results of the analysis of control assessment and monitoring information [CA-7 (f)]
* Monthly Reporting the security and privacy status of the system to {Insert Company Name} Technology Team and, when appropriate, to the AO or other client officials [CA-7 (g)]
* Independent assessors or assessment teams to monitor the security controls in the information system on an ongoing basis [CA-7 (1)]
* Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: [CA-7 (4)]
  + Effectiveness monitoring
  + Compliance monitoring
  + Change monitoring

8.8 Penetration Testing [CA-8, CA-8 (1,2)]

Once an Information System has been awarded an Authorized status, {Insert Company Name} must conduct penetration testing at least annually on specified components [CA-8] and must use an independent penetration agent or penetration team to perform penetration testing on the information system or system components. [CA-8 (1)]

{Insert Company Name} must employ red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement. The red-team exercises must be in alignment with the *StateRAMP Penetration Test Guidance*. [CA-8 (2)]

8.9 Internal System Connections [CA-9]

Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

{Insert Company Name} must:

* Authorize internal connections of components to the system [CA-9 (a)]
* Document each internal connection, the interface characteristics, security requirements, and the nature of the information communicated [CA-9 (b)]
* Terminate internal system connections after they are no longer required [CA-9 (c)]
* Review each internal connection at least annually or when material changes occur [CA-9 (d)]