

{Insert Company Name}

Security Procedures

Security Assessment and Authorization [CA]

**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](#_Toc153451051)

[Table of Contents 2](#_Toc153451052)

[1 Introduction 3](#_Toc153451053)

[2 Purpose 3](#_Toc153451054)

[3 Scope 3](#_Toc153451055)

[4 Roles and Responsibilities 3](#_Toc153451056)

[5 Management Commitment 4](#_Toc153451057)

[6 Authority 5](#_Toc153451058)

[7 Compliance 5](#_Toc153451059)

[8 Procedural Requirements [CA-1] 6](#_Toc153451060)

[8.1 Security Assessments [CA-2] 6](#_Toc153451061)

[8.2 Leveraging Results from External Organizations [CA-2 (3)] 6](#_Toc153451062)

[8.3 Information System and Interconnections[CA-3] 6](#_Toc153451063)

[8.4 Plan of Action & Milestones [CA-5 6](#_Toc153451064)

[8.5 Security Authorizations [CA-6] 6](#_Toc153451065)

[8.6 Continuous Monitoring and Penetration Testing [CA-7, CA-8] 6](#_Toc153451066)

[8.7 Internal System Connections [CA-9] 7](#_Toc153451067)

# 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 Access Control 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 access control 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. |
| **Individual or Group** | **Role** | **Responsibility** |
|  | 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.

# Procedural Requirements [CA-1]

The following security assessment and authorizations 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.

8.1 Security Assessments [CA-2]

{Insert Company Name} must contract with an American Association for Laboratory Accreditation (A2LA authorized Third Party Assessment Organization (3PAO) or) to conduct the needed assessment. [CA-2 (a)] The Information Security Team and the designated third party shall develop a Security Assessment Plan (SAP) as part of the security assessment process. [CA-2 (b)] {Insert Company Name} and the 3PAO shall create the following components for the SAP:

* A section documenting the security controls and control enhancements under assessment [CA-2 (b) (1)]
* Procedures that will be employed to determine the effectiveness of security controls [CA-2 (b) (2)]
* Documentation that articulates the assessment environment, assessment team, and assessment roles and responsibilities [CA-2 (b) (3)]

The SAP is reviewed and approved by the Authorizing Official or designated representative prior to conducting the assessment. [CA-2 (c)]

{Insert Company Name} ensures that the controls in the {Insert Product Name} Information System are assessed at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. [CA-2 (d)]

All documented security controls will be assessed annually by an accredited external third party using standardized testing methods to validate the secure functionality of all controls. [CA-2 (1)] A security assessment report will be created upon the completion of a security controls assessment. {Insert Company Name} will ensure that the report contains all the assessment results and provide adequate confidentiality for the document, given the sensitive nature of the content. [CA-2 (e)]

{Insert Company Name} ensures that security assessment reports are made available to authorized agency representatives by a secure methodology. If a control is discovered to be non-compliant or is not operating as intended, these deficiencies are identified in the assessment report and are also documented as a Plan of Actions & Milestones (POA&M) finding.

Annual security control assessment must include announced vulnerability scanning and in-depth monitoring and/or malicious user testing and/or insider threat assessment and/or performance/load testing and/or other defined security assessments. {Insert Company Name} management will accept the results of the assessment performed by the assessment team, and the results will be provided to the Information Security Team, the StateRAMP PMO, and the customer Authorizing Official (AO). [CA-2 (f)]

8.2 Leveraging Results from External Organizations [CA-2 (3)]

In order for {Insert Company Name} to leverage external organizations’s control assessment results provided by an accredited 3PAO The Information Security Team must do the following: [CA-2 (3)]

* Visit StateRAMP Marketplace by navigating to <https://StateRAMP.org/>
* Validate the organization’s status by navigating to the corresponding listing
* Obtain the Package ID from the listing to reference
* Reference the Package ID detailing the inherited control in the {Insert Product Name} Information System SSP where appropriate

8.3 Information System and Interconnections[CA-3]

{Insert Company Name} will develop Interconnection Security Agreements (ISA) or similar artifacts to authorize and document all system interconnections with third parties requiring access to data and authorized by the client. The {Insert Company Name} Information Security Team will review and update all Interconnection Security Agreements annually [CA-3 (c)]. These agreements will outline the rules of behavior and controls for the connection and include: [CA-3 (b)]

* The level and method of interconnection
* Impact on existing infrastructure and operations
* Hardware and software requirements
* Data sensitivity and user community
* Services and applications
* Security applications and controls
* Segregation of duties
* Incident reporting and response
* Contingency planning
* Data element naming and ownership
* Data backup
* Change management
* Rules of behavior
* Security training and awareness
* Roles and responsibilities
* Scheduling
* Cost and budgeting

The direct connection of any system to an external network without the use of the boundary protections that meet Trusted Internet Connection (TIC) requirements is prohibited. {Insert Company Name} employs deny-all, permit by exception policies for the information systems to connect to and exchange data with external information systems. All {Insert Company Name} interconnections are approved and managed in accordance with the Interconnection Security Agreements which must be approved by the Information Security Manager. [CA-3 (a)]

{Insert Company Name} authorizes internal connections of components required to operate and support the information system through Configuration Management Review and Security Assessment Review. Each internal connection, the interface characteristics, security requirements, and nature of the information communicated are documented in the information system baseline and System Communication Policy.

8.4 Plan of Action & Milestones [CA-5

Based on the results of assessments and monitoring, {Insert Company Name} will create actionable Plans of Action & Milestones (POA&M) in order to track remediation of the {Insert Product Name} Information System to a secure state. The Information Security Team will update and submit the POA&M at least monthly or during planned activities, such as security control assessments or a security impact analysis. [CA-5 (a)]

Updates to the POA&M may also be done when remediation is complete and the testing of the implemented security control meets the acceptable criteria to support a control being in place and operating as intended. A POA&M closure artifact must be created monthly to memorialize the evidence for closure. An example of a POA&M closure artifact would be a report from Qualys Policy Compliance or Qualys VMDR showing the non-compliance or vulnerability being remediated. [CA-5 (b)]

8.5 Security Authorizations [CA-6]

{Insert Company Name} has appointed a senior level executive or manager to the role of Designated Approving Authority (DAA) as the Authorizing Official (AO) for the {Insert Product Name} Information System and for common controls available for inheritance by organization systems. [CA-6 (a)] [CA-6 (b)] The designated Official will be:

* Appointed officially in writing
* Properly trained and qualified prior to acting in this role
* Proactively supported by {Insert Company Name} senior management

In order to operate the {Insert Product Name} Information System online, the AO must:

* Accept the use of common controls inherited by the system [CA-6 (c) (1)]
* Authorize, in writing, the {Insert Product Name} Information System [CA-6 (c) (2)]
* Authorizes the use of those controls for inheritance by organizational systems [CA-6 (d)]
* Ensure the {Insert Product Name} Information System is reaccredited (security authorization is updated), annually or when a significant change occurs. [CA-6 (e)]

8.6 Continuous Monitoring and Penetration Testing [CA-7, CA-8]

{Insert Company Name} has defined a Continuous Monitoring strategy for the {Insert Product Name} Information System that [CA-7]:

* Establish metrics that articulate the {Insert Product Name} Information System’s current security posture, detects adverse changes in the environment, and monitors control effectiveness to assist with operating the information system within acceptable risk levels. [CA-7 (a)]
* Assesses the information system and provides a configuration management process for the information system and its constituent components that is managed by the Configuration Management Board
* At least monthly, monitors control effectiveness for operating systems, databases, and web applications [CA-7 (b)]
* Facilitates annual third-party assessments of control effectiveness [CA-7 (b)]
* Assesses security controls throughout the lifecycle of the information system and documents any findings as a POA&M, which includes plans on how to address those findings [CA-7 (f)]
* Outlines ongoing security control assessments, and ongoing security status monitoring of defined metrics in accordance with the continuous monitoring strategy [CA-7 (c)] [CA-7 (d)]
* Outlines the correlation and analysis of security-related information generated by assessments and monitoring [CA-7 (e)]
* Outlines patch management and policy compliance remediation actions according to established timelines to address the results of the analysis of security-related information [CA-7 (f)]
* Reports the security state of the information system monthly to the {Insert Company Name} Technology Team, and to the AO or other client officials when appropriate [CA-7 (g)]
* Ensures risk monitoring is an integral part of the continuous monitoring strategy. This strategy includes monitoring: [CA-7 (4)]
  + Effectiveness of the implemented risk response measures
  + Compliance by verifying that required risk response measures are implemented and that security and privacy requirements are satisfied
  + Change by identifying deviations to the information system and in environments of operation that may affect security and privacy risk

{Insert Company Name} will employ independent FedRAMP approved Third Party Assessment Organization (3PAO) assessors or assessment teams to monitor the security controls in the information system on an ongoing basis. [CA-7 (1)] Additional, if needed, independent and accredited assessors will conduct penetration testing at least annually on all components within the information system boundary. [CA-(8)] [CA-8 (1)] {Insert Company Name} utilizes KnowBe4 to conduct red-team exercises. These red-team exercises are synthetic phishing campaigns and are run weekly. The KnowBe4 phishing campaigns simulate attempts by adversaries to compromise the {Insert Product Name} Information System. [CA-8 (2)]

8.7 Internal System Connections [CA-9]

The Information Security Team has authorized the internal connections to the {Insert Product Name} Information System. [CA-9 (a)] {Describe authorized internal connections for remote access/remote desktop.} Additionally, the Information Security Team has authorized the use of {Insert list of authorized management products} from the management subnet within the authorization boundary. [CA-9 (b)] The internal connections are documented in the Network Diagrams, Data Flow Diagrams, and within the SSP. {Insert Company Name} will terminate internal system connections to the {Insert Product Name} Information System after they are no longer required, [CA-9 (c)] and will review each internal connection at least annually or when material changes occur. [CA-9 (d)]