Insert Logo Here

Organization Name

Security Procedure

Security Assessment & Authorization

Version 1.0

April 6, 2021

Proprietary and Confidential

For Authorized Use Only

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 4/6/2021 | 1.0 | Published CA Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68599589)

[2 Purpose 1](#_Toc68599590)

[3 Scope 1](#_Toc68599591)

[4 Roles and Responsibilities 1](#_Toc68599592)

[5 Management Commitment 2](#_Toc68599593)

[6 Authority 3](#_Toc68599594)

[7 Compliance 3](#_Toc68599595)

[8 Procedural Requirements 4](#_Toc68599596)

[8.1 Security Assessments 4](#_Toc68599597)

[8.2 Information System and Interconnections 4](#_Toc68599598)

[8.3 Plan Of Action & Milestones 5](#_Toc68599599)

[8.4 Security Authorizations 5](#_Toc68599600)

[8.5 Continuous Monitoring and Penetration Testing 5](#_Toc68599601)

# Introduction

 has developed procedures that identify the security requirements for its information systems and personnel to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by management and in compliance with the Security Assessment & Authorization family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

# Purpose

This document defines the information security assessment and authorization procedures. These procedures are in place to facilitate the implementation of the Security Assessment and Authorization Policy and associated access controls. In accordance with the policy, these procedures detail how information shall implement and maintain secure access controls on all applicable information systems.

# Scope

The provisions of these policies pertain to all employees, contractors, third parties, and others who have access to company and customer confidential information within systems and facilities.

# Roles and Responsibilities

These policies apply to all employees, contractors, business partners, third parties, and others who need or have access to systems and our customer's confidential information.

| **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 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. |
|  | 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 Manager | 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 Administrator | Responsible for conducting information system security Administration activities. |
|  | Managers | Responsible for understanding, enforcing, and complying with control requirements defined in Policies and Procedures |
|  | Users | Responsible for understanding and complying with Policies and Procedures. |

# Management Commitment

 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 system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the 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/Federal Information Security Management Act of 2002 (FISMA)
2. The Privacy Act of 1974
3. Clinger-Cohen Act of 1996
4. OMB Circulars and Memoranda
5. Federal Information Processing Standards (FIPS)
6. NIST Special Publications
7. OMB Memorandum for Chief Information Officers and Chief Acquisition Officers: Ensuring New Acquisitions Include Common Security Configurations, June 2007
8. 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 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 annually by an external vendor 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

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 Organization Name information systems.

## Security Assessments

The {Role} and the designated third party shall develop a Security Assessment Plan (SAP) as part of the security assessment process. Organization Name shall create the following components for the SAP:

* A section documenting the security controls and control enhancements under assessment
* Procedures that will be employed to determine the effectiveness of security controls
* Documentation that articulates the assessment environment, assessment team, and assessment roles and responsibilities

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. A security assessment report will be created upon the completion of a security controls assessment. Organization Name will ensure that the report contains all of the assessment results and provide adequate confidentiality for the document, given the sensitive nature of the content.

Organization Name shall ensure that security assessment reports are made available to the agency Security Officer by secure file transfer. If a control is discovered to be non-compliant or is not operating as intended, these deficiencies are identified in the assessment report and they are also documented as POA&M issues.

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. Organization Name upper management will accept the results of the assessment performed by the appropriate assessor.

## Information System and Interconnections

Organization Name will develop Interconnection Security Agreements and utilize them to authorize and document all system interconnections with third parties requiring access to data and authorized by the client. The Organization Name {Role} will review and update all Interconnection Security Agreements annually. These agreements will outline the rules of behavior and controls for the connection and include:

* 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. Organization Name employs deny-all, permit by exception policies for the information systems to connect to and exchange data with external information systems. All Organization Name interconnections operate in accordance with the Interconnection Security Agreements which must be approved by the {Role}

Organization 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.

## Plan Of Action & Milestones

Based on the results of assessments and monitoring, Organization Name will create actionable plans of action and milestones to remediate systems to a secure state. The {Role/Team} will update the POA&M at least monthly or during planned activities, such as security control assessments or a security impact analysis.

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.

## Security Authorizations

Organization Name must appoint a senior level executive or manager to the role of Designated Approving Authority (DAA) as the Authorizing Official. The designated Official will be:

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

To operate any Organization Name information system online, the information system owner must ensure that:

* The Authorizing Official has authorized, in writing, the operation of the information system
* The information system is reaccredited (security authorization is updated), at least every three years or when a significant change occurs.

## Continuous Monitoring and Penetration Testing

Organization Name will define a Continuous Monitoring Strategy for the information system that will:

* Assess the information system and develop a configuration management process for the information system and its constituent components that is managed by the Configuration Management Board
* Monitor operating systems, databases, web applications, and facilitate annual third-party assessments of monitoring activities on an annual basis
* Assess security controls throughout the lifecycle of the information system and document any findings within the POA&M
* Outline ongoing security status monitoring of defined metrics in accordance with the continuous monitoring strategy and the correlation and analysis of security-related information generated by assessments and monitoring
* Outline patch management actions according to StateRAMP timelines to address the results of the analysis of security-related information
* Report the security state of the information system to the appropriate security office

Organization Name will employ assessors or assessment teams with an independent level of assessment to monitor the security controls in the information system on an ongoing basis. Additional independent and accredited assessors will conduct penetration testing at least annually on all components within the information system boundary.