Insert Logo Here

Organization Name

Security Procedure

Risk Assessment

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 RA Procedure | Noah Brown, CISO |

Table of Contents

[1 Introduction 1](#_Toc68608796)

[2 Purpose 1](#_Toc68608797)

[3 Scope 1](#_Toc68608798)

[4 Roles and Responsibilities 1](#_Toc68608799)

[5 Management Commitment 2](#_Toc68608800)

[6 Authority 3](#_Toc68608801)

[7 Compliance 3](#_Toc68608802)

[8 Procedural Requirements 4](#_Toc68608803)

[8.1 Security Categorization 4](#_Toc68608804)

[8.2 Risk Assessments 4](#_Toc68608805)

[8.3 Vulnerability Scanning 5](#_Toc68608806)

# Introduction

Organization Name 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 Organization Name management and in compliance with the Risk Assessment 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 risk assessment procedures. These procedures are in place to facilitate the implementation of the Risk Assessment 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 Organization Name employees, contractors, third parties, and others who have access to company and customer confidential information within Organization Name systems and facilities.

# Roles and Responsibilities

These policies apply to all Organization Name employees, contractors, business partners, third parties, and others who need or have access to Organization Name 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 Organization 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. |
|  | 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

Organization 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 Organization Name system by implementing adequate security controls.

# Authority

These policies and procedures are issued under the authority of the Organization 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/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 Organization Name 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 risk assessment 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 Categorization

Organization Name will categorize information and information systems in accordance to applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance and NIST Special Publication SP 800-53. Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type.

Security categorization results and the supporting rationale must always be documented in *Security Assessment Plan* and subsequent report and the {Team/Role} will review and approve the security categorization decision.

## Risk Assessments

The {Team/Role} is responsible for identifying critical assets that support the business by rating each asset as Low, Medium, or High. Risk assessments include the likelihood and magnitude of harm resulting from the following items or events:

* Unauthorized access
* Unauthorized use
* Unauthorized disclosure
* Unauthorized disruption
* Unauthorized modification
* Unauthorized destruction
* Transmission anomalies

The {Team/Role} is also responsible for identifying natural and man-made threats and assigning a ranking of Low, Medium, or High.

The {Team/Role} is responsible for documenting the results of the risk assessment in the *StateRAMP Risk Assessment Report* and reviewing the risk assessment results every three (3) years or when there are significant changes to the operating environment occur. Risk assessment results are disseminated to designated StateRAMP ISO and the {Team/Role} will:

* Review risk assessment results in relation to current POA&M progression
* Identify findings that are no longer applicable
* Call out points of interest for the next risk assessment and define progress metrics

## Vulnerability Scanning

Organization Name employs SCAP Commercial-off-the-Shelf (COTS) vulnerability scanning tools {Tools} that include the capability to readily update the list of vulnerabilities scannedto scan the information systems.

A formal schedule for conducting vulnerability scans at least monthly has been developed and implemented for operating systems and infrastructure and monthly for web applications and databases. These scans are performed by the {Team/Role} and include all information system components and applications within the system boundary.

An accredited independent assessor must scan Organization Name operating systems, infrastructure, web applications, and databases annually. Vulnerability scanning tools and techniques shall be employed by the {Team/Role} to promote interoperability features among tools and automate parts of the vulnerability management process.

The {Team/Role} is responsible for defining standards for:

* Enumerating platforms, software flaws, and improper configurations
* Formatting checklists and test procedures
* Measuring vulnerability impact using {Tools} severity levels one (1) through five (5)

The {Team/Role} will ensure the scan software updates the list of information system vulnerabilities prior to a new scan or when there are new vulnerabilities identified and reported and all vulnerabilities identified in a risk assessment are analyzed, documented, and addressed based on accepted risk practices.

Vulnerabilities will be remediated based off of {Tool} severity level. Remediation of identified risks is performed within:

* Thirty (30) days for High-Risk vulnerabilities ({Tool} severity levels 4 and 5)
* Ninety (90) days for Moderate-Risk vulnerabilities ({Tool} severity levels 2 and 3)
* One Hundred and Eighty (180) Days for Low-Risk vulnerabilities ({Tool} severity level 1)

The results of the vulnerability scans are communicated to the designated StateRAMP ISSO. The Information Security Team shall:

* Review scan results for official internal distribution
* Ensure results are available only to relevant personnel

Organization Name must use vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. All vulnerability scanning tools and techniques shall be employed by the {Team/Role}to cover all components that are defined within the boundary of the information and produce details needed regarding each component scanned and the vulnerabilities that each component was checked against. {Tools} vulnerability libraries are updated as new vulnerabilities are identified.

Organization Name information system will allow controlled privileged access authorization to operating systems, infrastructure, databases, and web applications for specific service accounts solely for vulnerability scanning activities in order to facilitate more thorough scanning.

{Tools} will be used to analyze and perform trend analysis every thirty (30) days on the vulnerabilities scans that are conducted. All critical and high findings merit a historic review of all audit logs to determine if the vulnerability has been previously exploited.