

{Insert CompanY Name}

Security Procedures

Risk Assessment (RA)

**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](#_Toc153292702)

[Table of Contents 2](#_Toc153292703)

[1 Introduction 3](#_Toc153292704)

[2 Purpose 3](#_Toc153292705)

[3 Scope 3](#_Toc153292706)

[4 Roles and Responsibilities 3](#_Toc153292707)

[5 Management Commitment 4](#_Toc153292708)

[6 Authority 5](#_Toc153292709)

[7 Compliance 5](#_Toc153292710)

[8 Procedural Requirements [RA-1] 6](#_Toc153292711)

[8.1 Security Categorization [RA-2] 6](#_Toc153292720)

[8.2 Risk Assessments [RA-3, RA-3 (1)] 6](#_Toc153292721)

[8.3 Vulnerability Scanning [RA-5, RA-5 (2), RA-5 (3), RA-5 (5), RA-5 (11)] 7](#_Toc153292722)

[8.4 Risk Response [RA-7] 8](#_Toc153292723)

[8.5 Criticality Analysis [RA-9] 9](#_Toc153292724)

# 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 [RA-1]

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 {Insert Company Name} information systems.



## Security Categorization [RA-2]

{Insert Company Name} categorizes information and information systems in accordance to applicable Federal and State laws, Executive Orders, directives, policies, regulations, standards, guidance, and NIST Special Publications. [RA-2 (a)] 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 are documented in the *Security Assessment Plan* [RA-2 (b)] and subsequent report and the {Insert Information Security Team Name} will review and approve the security categorization decision. [RA-2 (c)]

## Risk Assessments [RA-3, RA-3 (1)]

The {Insert Information Security Team Name} is responsible for identifying assets that support the business and rating each asset as Low, Medium, or High impact. Risk assessments includes: [RA-3 (a)]

* Identifying threats to and vulnerabilities in the system [RA-3 (a) (1)]
* Determining the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits and any related information [RA-3 (a) (2)]
* Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information [RA-3 (a) (3)]

After the Risk Assessment is complete, the {Insert Information Security Team Name}:

* Integrates risk assessment results and risk management decisions from the organization mission or business process perspectives with system-level risk assessment. [RA-3 (b)]
* Documents risk assessment results in a security assessment report [RA-3 (c)]
* Reviews the risk assessment results at least annually [RA-3 (d)]
* Disseminates the risk assessment report to the Information Owner, {Insert Information Security Team Name} Manager, and Authorizing Official (AO) [RA-3 (e)]
* Updates the risk assessment at least annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security and privacy state of the system. [RA-3 (f)]

The {Insert Information Security Team Name} is also responsible for identifying natural and man-made threats and assigning a ranking of Low, Medium, or High impact and likelihood.

The {Insert Information Security Team Name} 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 program Information System Security Officer or upon request. The {Insert Information Security Team Name} will:

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

{Insert Company Name} must assess supply chain risks associated with the {Insert Product Name} Information System, system components and system services by utilizing the Cybersecurity Supply Chain Risk Management (SCRM) Plan. [RA-3 (1) (a)] The supply chain risk assessment must be updated at least annually, when there are significant changes to the relevant supply chain, when there are significant changes to the system, when there are significant changes to environments of operation, or other conditions that may necessitate a change in the supply chain. [RA-3 (1) (b)]

## Vulnerability Scanning [RA-5, RA-5 (2), RA-5 (3), RA-5 (5), RA-5 (11)]

NOTE: Scanning must be accomplished using a Security Content Automation Protocol (SCAP) tool validated by the National Institute of Standards and Technology (NIST), The list of validated tools can be found at <https://csrc.nist.gov/Projects/scap-validation-program/Validated-Products-and-Modules>.

{Insert Company Name} employs SCAP Commercial-off-the-Shelf (COTS) vulnerability scanning tools ({Insert list of SCAP approved tools utilized}) 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, or after new vulnerabilities potentially affecting the system are identified and reported, has been developed and implemented for operating systems, infrastructure, web applications, and databases. [RA-5 (a)] These scans are performed by the {Insert Information Security Team Name} and include all information system components (including new components) and applications within the system authorization boundary.

An accredited independent assessor must scan {Insert Company Name}’s operating systems, infrastructure, web applications, and databases annually. Vulnerability scanning tools and techniques are employed by the {Insert Information Security Team Name} to promote interoperability features among tools and automate parts of the vulnerability management process. [RA-5 (b)]

The {Insert Information Security Team Name} is responsible for defining standards for:

* Enumerating platforms, software flaws, and improper configurations [RA-5 (b) (1)]
* Formatting checklists and test procedures [RA-5 (b) (2)]
* Measuring vulnerability impact using {Insert Vulnerability Scanning Tool Name} severity levels mapped to StateRAMP standard vulnerability levels (Low, Moderate, High) [RA-5 (b) (3)]

The {Insert Information Security Team Name} ensures the scan software updates the list of information system vulnerabilities prior to a new scan and all vulnerabilities identified in a risk assessment are analyzed, documented, and addressed based on accepted risk practices. Any false positive findings are tracked and documented by the {Insert Information Security Team Name} with the supporting rationale. All remaining legitimate findings are added to the {Insert Product Name} POA&M spreadsheet. [RA-5 (c)]

Vulnerabilities will be remediated based on {Insert Vulnerability Scanning Tool Name} severity level. Remediation of identified risks is performed within: [RA-5 (d)]

* Thirty (30) days for High-Risk vulnerabilities
* Ninety (90) days for Moderate-Risk vulnerabilities
* One Hundred and Eighty (180) Days for Low-Risk vulnerabilities

NOTE: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog ([https://www.cisa.gov/known-exploited vulnerabilities-catalog](https://www.cisa.gov/known-exploited%20vulnerabilities-catalog)) the KEV remediation date should supersede the StateRAMP parameter requirement.

The results of the vulnerability scans are communicated to the {Insert Company Name} Technology Team and the Authorizing Official. The {Insert Information Security Team Name} shall: [RA-5 (e)]

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

{Insert Company Name} uses vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. [RA-5 (f)] All vulnerability scanning tools and techniques employed by the {Insert Information Security Team Name} cover all components that are defined within the boundary of the information system and produce details needed regarding each component scanned and the vulnerabilities that each component was checked against. [RA-5 (3)] {Insert Vulnerability Scanning Tool Name} vulnerability libraries are updated as new vulnerabilities are identified. {Insert Vulnerability Scanning Tool Name} automatically updates the list of information system vulnerabilities multiple times per day. [RA-5 (2)] The {Insert Product 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 to facilitate more thorough scanning. [RA-5 (5)]

The public can disclose discovered vulnerabilities regarding the {Insert Product Name} Information System to {Insert Company Name} via the publicly available {Insert Product Name} Web Application support portal. [RA-5 (11)]

{Insert Vulnerability Scanning Tool Name} 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.

## Risk Response [RA-7]

{Insert Company Name} addresses the need to determine an appropriate response to risk before generating a Plan of Action and Milestones (POA&M) entry. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a POA&M entry is not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a POA&M entry is generated to track the mitigation of the entry.

## Criticality Analysis [RA-9]

{Insert Company Name} performs criticality analysis when an architecture or design is developed, modified, or upgraded. If such analysis is performed early in the system development life cycle, {Insert Company Name} may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design. Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-2.