

{Insert Company Name}

Security Policy

Risk Assessment

**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

1 Introduction ............................................................................................................................................. 1

2 Purpose .................................................................................................................................................... 1

3 Scope ........................................................................................................................................................ 2

4 Roles and Responsibilities ........................................................................................................................ 2

5 Management Commitment ..................................................................................................................... 2

6 Authority .................................................................................................................................................. 3

7 Compliance .............................................................................................................................................. 3

8 Policy Requirements ................................................................................................................................ 4

8.1 Risk Assessment Policies and Procedures [RA-1] ............................................................................. 4

8.2 Security Categorization [RA-2] ......................................................................................................... 4

8.3 Risk Assessment [RA-3, RA-3 (1)] ..................................................................................................... 6

8.4 Vulnerability Monitoring and Scanning [RA-5, RA-5 (2,3,5,11), {RA-5 (4,8) High Only}] .................. 6

8.5 Risk Response [RA-7] ....................................................................................................................... 6

8.6 Criticality Analysis [RA-9] ................................................................................................................. 6

# 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.

# Policy Requirements

The following personally identifiable information processing and transparency 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}.

The following access control requirements, mechanisms, and provisions are to be followed by all employees, management, contractors, and other users who access and support the {Insert Company/Product Name} information systems.

8.1 Risk Assessment Policies and Procedures [RA-1]

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

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

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

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

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

8.2 Security Categorization [RA-2]

{Insert Company Name} must categorize each system and information it processes, stores, and transmits in accordance with applicable Federal and State Laws, Executive Orders, directives, policies, regulations, standards, and guidance. [RA-2 (a)] All security categorization results, including supporting rationale, are included in the security plan [RA-2 (b)] and all security categorization decisions must be reviewed and approved by the Authorizing Official or authorizing official designated representative. [RA-2 (c)]

8.3 Risk Assessment [RA-3, RA-3 (1)]

{Insert Company Name} must conduct an internal assessment to: [RA-3 (a)]

* + Identify threats to and vulnerabilities in the system [RA-3 (a) (1)]
  + Determine 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)]
  + Determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information [RA-3 (a) (3)]
  + Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessment [RA-3 (b)]
* Document risk assessment results in a security assessment report [RA-3 (c)]
* Review the risk assessment results at least annually [RA-3 (d)]
* Disseminate the risk assessment report to the Information Owner, Information Security Manager, and Authorizing Official (AO) [RA-3 (e)]
* Update 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)]

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

8.4 Vulnerability Monitoring and Scanning [RA-5, RA-5 (2,3,5,11), {RA-5 (4,8) High Only}]

{Insert Company Name} must:

* Monitor and scan for vulnerabilities in the system and hosted applications no less than monthly or after new vulnerabilities potentially affecting the system are identified and reported [RA-5 (a)]
* Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automated parts of the vulnerability management process by standards for: [RA-5 (b)]
  + Enumerating platforms, software flaws, and improper configurations [RA-5 (b) (1)]
  + Formatting checklists and test procedures [RA-5 (b) (2)]
  + Measuring vulnerability impact [RA-5 (b) (3)]
* Analyze vulnerability scan reports and results from vulnerability monitoring [RA-5 (c)]
* Remediate legitimate vulnerabilities (180 days for Low, 90 days for Medium, 30 days for High) in accordance with an organizational assessment of risk [RA-5 (d)]
* Share information obtained from the vulnerability monitoring process and control assessment with the {Insert Company Name} Technology Team and Authorizing Officials to help eliminate similar vulnerabilities in other systems [RA-5 (e)]
* Employ vulnerabilities monitoring tools that include the capability to readily update the vulnerabilities to be scanned [RA-5 (f)]

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>.

To conduct the monthly and ad hoc vulnerability scans, the information security team must:

* Update the system vulnerabilities to be scanned within 24 hours prior to each new scan, or when new vulnerabilities are identified and reported [RA-5 (2)]
* Employ vulnerability scanning procedures that define the breadth and depth of vulnerability scanning coverage [RA-5 (3)]
* Implement privileged access authentication to all components that support authentications and to all scans for credentials to operating systems, infrastructure, database, and web applications for all vulnerability scans to facilitate more thorough scanning [RA-5 (5)]
* Establish a public reporting channel for receiving reports of vulnerabilities in systems and system components [RA-5 (11)]

**For high impact systems only:**

* Determine information about the system that is discoverable, and notify appropriate services provider personnel and follow procedures for organization and service provider-defined corrective actions [RA-5 (4)]
* Review historic audit logs to determine if a high or critical vulnerability identified in the information system has been previously exploited within the last year [RA-5 (8)]

If the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a plan of action and milestones entry is generated.

8.5 Risk Response [RA-7]

{Insert Company Name} must respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. [RA-7]

8.6 Criticality Analysis [RA-9]

{Insert Company Name} must identify critical system components and functions by performing a criticality analysis for systems, system components, or system services of the operational environment that could impact the criticality of the development, material modification, or major upgrade. [RA-9]