

{Insert Company Name}

Security Policy

Supply Chain Risk Management

**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 Supply Chain Risk Management Policies and Procedures [SR-1] ..................................................... 4

8.2 Supply Chain Risk Management Plan [SR-2, SR-2 (1)] ...................................................................... 4

8.3 Supply Chain Controls and Processes [SR-3] .................................................................................... 5

8.4 Acquisition Strategies, Tools, and Methods [SR-5] .......................................................................... 5

8.5 Supplier Assessments and Reviews [SR-6] ....................................................................................... 5

8.6 Notification Agreements [SR-8] ....................................................................................................... 5

8.7 Tamper Resistance and Detection [{SR-9, SR-9 (1) High Only}] ........................................................ 5

8.8 Inspection of Systems or Components [SR-10] ................................................................................ 5

8.9 Component Authenticity [SR-11, SR-11 (1,2)] .................................................................................. 5

8.10 Component Disposal [SR-12] .......................................................................................................... 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}’ 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}’ 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}’ 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}’ 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 Supply Chain Risk Management Policies and Procedures [SR-1]

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

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

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

{Insert Company Name} must review and update the current supply chain risk management: [SR-1 (c)]

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

8.2 Supply Chain Risk Management Plan [SR-2, SR-2 (1)]

{Insert Company Name} must develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of its information systems. [SR-2 (a)]

{Insert Company Name} must review and update the supply chain risk management plan at least annually, or as required, to address threats, organizational changes, or environmental changes. [SR-2 (b)]

{Insert Company Name} must protect the supply chain risk management plan from unauthorized disclosure and modification. [SR-2 (c)]

{Insert Company Name} must establish a supply chain risk management team consisting of key stakeholders to lead and support the SCRM activities. [SR-2 (1)]

8.3 Supply Chain Controls and Processes [SR-3]

{Insert Company Name} must establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of system and system components in coordination with supply chain personnel. [SR-3 (a)]

{Insert Company Name} must employ controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events. [SR-3 (b)]

The {Insert Company Name} Chief Information Security Officer (CISO) is responsible for the documentation and maintenance of the supply chain custody, including replacement devices, to ensure the integrity of the devices being introduced to the boundary. [SR-3 (c)]

8.4 Acquisition Strategies, Tools, and Methods [SR-5]

{Insert Company Name} must employ acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risk.

8.5 Supplier Assessments and Reviews [SR-6]

{Insert Company Name} must assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system services they provide at least annually.

8.6 Notification Agreements [SR-8]

{Insert Company Name} should establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessment of audits of {Insert Company Name} data. CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.

8.7 Tamper Resistance and Detection [{SR-9, SR-9 (1) High Only}]

**For high impact systems only:**

{Insert Company Name} must implement a tamper protection program for the system, system component, or system service. [SR-9] {Insert Company Name} must employ anti-tamper technologies, tools, and techniques throughout the system development life cycle. [SR-9 (1)]

8.8 Inspection of Systems or Components [SR-10]

{Insert Company Name} must inspect operating systems at random, upon installation of new system components, and/or upon any indication of tampering with systems or system components.

8.9 Component Authenticity [SR-11, SR-11 (1,2)]

{Insert Company Name} must develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. [SR-11 (a)]

{Insert Company Name}’ Information Security Team must report counterfeit system components to the source of the counterfeit component, government law enforcement agencies, the manufacturers of the component, and/or external agencies if deemed necessary. [SR-11 (b)]

The {Insert Company Name} Technology Team must be trained to detect counterfeit system components to include hardware, software, and firmware. [SR-11 (1)]

{Insert Company Name} must maintain configuration control over all system components awaiting service or repair and serviced or any components awaiting return to service. [SR-11 (2)]

8.10 Component Disposal [SR-12]

{Insert Company Name} must dispose of data, documentation, or system components that retain data by using one or more of the following techniques and methods: degaussing, shredding, incineration, and/or crushing systems or system components. Procedures must be consistent with NIST SP 800-88.