

{Insert CompanY Name}

Security Procedures

Supply Chain Risk Management [SR]

**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](#_Toc152925467)

[Table of Contents 2](#_Toc152925468)

[1 Introduction 3](#_Toc152925469)

[2 Purpose 3](#_Toc152925470)

[3 Scope 3](#_Toc152925471)

[4 Roles and Responsibilities 3](#_Toc152925472)

[5 Management Commitment 4](#_Toc152925473)

[6 Authority 5](#_Toc152925474)

[7 Compliance 5](#_Toc152925475)

[8 Procedural Requirements [SR-1] 6](#_Toc152925476)

[8.1 Supply Chain Risk Management Plan [SR-2, SR-2 (1)] 6](#_Toc152925477)

[8.2 Supply Chain Controls and Processes & Acquisition Strategies, Tools, and Methods [SR-3, SR-5] 6](#_Toc152925478)

[8.3 Supplier Assesment and Reviews [SR-6] 6](#_Toc152925479)

[8.4 Notification Agreements [SR-8] 6](#_Toc152925480)

[8.5 Inspection of Systems or Components [SR-10] 7](#_Toc152925481)

[8.6 Component Authenticity [SR-11, SR-11 (1, 2)] 7](#_Toc152925482)

[8.7 Component Disposal [SR-12] 7](#_Toc152925483)

# Introduction

{Insert Company Name} has developed corporate procedures that identify the security requirements for its information systems and personnel in order to ensure the integrity, confidentiality, and availability of its information. These procedures are set forth by {Insert Company Name}’s management and in compliance with the Supply Chain Risk Management family of controls found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.

# Purpose

The purpose of these procedures is to establish supply chain risk management requirements to ensure the confidentiality, integrity, and availability of {Insert Company Name}’s systems, facilities, and data are protected. These procedures are consistent with applicable state and federal laws, Executive Orders, directives, regulations, standards, and guidance.

# Scope

The provisions of these procedures 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 procedures 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** |
| {Insert Individual Name} | CEO | Highest-level official with overall responsibility to develop, implement, and maintain accountability, active support, oversight, and management commitment for information security objectives. |
| {Insert Individual Name} | President | Responsible for developing, implementing, maintaining, and ensuring compliance with information security policies, procedures, and controls. Has final responsibility for information security program. |
| {Insert Individual Name} | 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. |
| **Individual or Group** | **Role** | **Responsibility** |
| {Insert Individual Name} | Authorizing Official | Responsible for operating information system at an acceptable level of risk to organizational operations and assets. |
| {Insert Individual Name} | Authorizing Official Designated Representative | Acts on behalf of Authorizing Official to coordinate and conduct day-to-day activities associated with security authorization process. |
| {Insert Individual Name} | 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. |
| {Insert Individual Name} | Information Security Manager | Responsible for conducting information system security engineering activities.  Responsible for providing for appropriate security, to include management, operational, and technical controls. |
| {Insert Individual Name} | Information Technology Director | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. |
| {Insert Individual Name} | 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. |
| {Insert Individual or Team Name} | 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 procedures 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 procedures 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 [SR-1]

The following identification and authentication 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.

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

{Insert Company Name} has created a Supply Chain Risk Management Plan (SCRMP) as Appendix P to the SSP, Supply Chain Risk Management Plan, version N.N. [SR-2 (a)] The SCRMP is reviewed and updated annually, and the updates are cataloged in the Document Revision Table. [SR-2 (b)] The SCRMP is only accessible to all authorized {Insert Information System Name} Information System personnel via the {Insert Documentation Repository Name}. [SR-2 (c)]

{Insert Company Name} established a Supply Chain Risk Management Team consisting of personnel from the {Insert Organizational Team Names}. A review of the security posture of any technology platform is integrated into the purchasing process. {Insert Organizational Team Name(s)} reviews the vendor’s security documentation and {Insert Organizational Team Name(s)} reviews the contract terms and conditions. {Insert Organizational Team Name(s)} ensures each review is completed before the new technology is purchased. {Insert Organizational Team Name(s)} tracks license counts and contract duration. [SR-2 (1)]

{Insert inherited control language if applicable}

8.2 Supply Chain Controls and Processes & Acquisition Strategies, Tools, and Methods [SR-3, SR-5]

{Insert Company Name} {Insert organization's procedures for purchasing external technology services} [SR-3 (a)] [SR-3 (b)] [SR-5] {Insert Company Name} has documented the selected and implemented supply chain processes and controls in its SCRMP. [SR-3 (c)]

{Insert inherited control language if applicable}

8.3 Supplier Assesment and Reviews [SR-6]

{Insert Company Name} assess and reviews the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide at the time of initial purchase, at any renewal point, and/or annually. This review may include reviewing the supplier’s SSP, their SOC2 report, or other relevant security documentation. [SR-6]

{Insert inherited control language if applicable}

8.4 Notification Agreements [SR-8]

{Insert Company Name} establishes agreements with suppliers involved in the supply chain for an acquired system, system component, or system service for the notification of potential supply chain compromises and/or results of assessment or audits. This can include reviewing the supplier’s SSP, their SOC2 report, or other relevant security documentation.

{Insert Company Name} monitors numerous advisory feeds including CISA Alerts, MS-ISAC, IC3, and {Insert Vendor(s) Name} security alerts. Ad-hoc scans are also performed on systems, system components, and corporate devices to verify proper updates are installed.

{Insert inherited control language if applicable}

8.5 Inspection of Systems or Components [SR-10]

{Insert Company Name} performs scans at random, upon installation of new system components, and/or upon any indication of tampering on systems, system components, and corporate devices to verify proper updates are installed. Scans are performed to verify that systems, system components, and corporate devices have not been tampered with. [SR-10]

{Insert inherited control language if applicable}

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

{Insert Company Name} {Insert organization's procedures for purchasing external technology services} [SR-11 (a)]

{Insert Company Name} reports suspected systems and/or system components to the source of the counterfeit component and the {Insert Role Name}. [SR-11 (b)]

{Insert Organizational Team, Role, or Individual Name(s)} has (have) been trained to detect counterfeit system components to include, hardware, software, and firmware. [SR-11 (1)]

{Insert inherited control language if applicable}

8.7 Component Disposal [SR-12]

{Insert Company Name} adheres to the NIST SP800-88 guidance for the disposal of data, documentation, tools, and system components. [SR-12] The NIST SP800-88 can be found at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

{Insert inherited control language if applicable}