City of Milwaukee

Supply Chain Risk Management Policy

NIST Reference: SR – Supply Chain Risk Management	Implementation Date : Draft	Revision Number : 1.0

Supply Chain Risk Management Policy

Purpose

The Supply Chain Risk Management (SCRM) Policy is established to ensure the resilience of the City of Milwaukee against potential security risks introduced through its supply chain. This policy aims to identify, assess, and mitigate risks associated with suppliers, vendors, and third-party partners. By implementing effective supply chain controls and processes, this policy safeguards the integrity, authenticity, and confidentiality of the organization's information systems, products, and services.

Scope

This Supply Chain Risk Management Policy applies to all facets of the City of Milwaukee's supply chain, encompassing goods, services, software, and components procured from external sources. It covers all departments, divisions, and branches of the organization involved in supply chain activities. The policy is applicable to all personnel engaged in supply chain management, procurement, and vendor selection processes.

Roles and Responsibilities

Management

The Management team holds ultimate accountability for the implementation, enforcement, and continuous improvement of this Supply Chain Risk Management Policy. They shall provide the necessary resources, support, and commitment to ensure effective supply chain risk management. Management oversees the overall strategy and alignment of supply chain risk management with the organization's goals. They also take on the responsibility of coordinating and executing supply chain risk management efforts, including risk assessments, supplier reviews, and formulation of mitigation strategies.

Information Security

The Information Security team, in collaboration with Management, is responsible for coordinating and executing supply chain risk management efforts. They contribute to supply chain risk assessments, identify potential security vulnerabilities, and recommend security controls. The Information Security team ensures compliance with security requirements during procurement processes. They also work closely with System Administrators to implement and monitor technical security measures.

System Administrators

System Administrators play a crucial role in implementing and maintaining the technical aspects of the Supply Chain Risk Management Policy. They ensure that IT systems and networks align with security requirements, including those related to supply chain risk management. System Administrators monitor and manage security measures, patches, and updates to mitigate potential vulnerabilities. They collaborate with both Management and Information Security to ensure technical systems are compliant and effectively contribute to risk management efforts.

SCRM

The SCRM Team is responsible for coordinating and executing supply chain risk management efforts, including risk assessments, supplier reviews, and mitigation strategies.

Purchasing

The Purchasing department shall assess suppliers' security capabilities, negotiate notification agreements, and implement supply chain controls during the acquisition process.

NIST security controls

SR-1 Policy and Procedures

The City of Milwaukee shall establish and maintain comprehensive policies and procedures for supply chain risk management. These documents shall define roles, responsibilities, and best practices related to identifying, assessing, and mitigating supply chain risks. Regular reviews and updates of these policies and procedures shall be conducted to reflect the evolving supply chain landscape and organizational requirements.

SR-2 Supply Chain Risk Management Plan

The City of Milwaukee shall develop and maintain a Supply Chain Risk Management Plan that outlines the approach for identifying, evaluating, and managing supply chain risks throughout the procurement lifecycle.

SR-2(1) Establish SCRM Team

A dedicated Supply Chain Risk Management (SCRM) Team shall be established, comprising representatives from Information Security, Procurement, Legal, and relevant departments. The SCRM Team shall be responsible for coordinating and executing supply chain risk management efforts.

SR-3 Supply Chain Controls and Processes

The City of Milwaukee shall implement appropriate supply chain controls and processes to verify the integrity, authenticity, and security of goods, services, software, and components acquired from external

sources.

SR-5 Response to Audit Logging Process Failures

The City of Milwaukee shall adopt acquisition strategies, tools, and methods that prioritize supply chain security and risk considerations. This includes evaluating potential suppliers' security postures and considering the use of reputable vendors with established security practices.

SR-8 Notification Agreements

Formal notification agreements will be established with suppliers to promptly inform the City of Milwaukee of any security incidents or supply chain disruptions that may impact the organization.

SR-10 Inspection of Systems or Components

The City of Milwaukee may conduct periodic inspections and audits of systems or components acquired from suppliers to verify compliance with security requirements and ensure the integrity of the supply chain.

SR-11 Component Authenticity

The City of Milwaukee shall implement measures to verify the authenticity of components used in its systems. This includes anti-counterfeit training for personnel involved in procurement and configuration control for component service and repair.

SR-12 Component Disposal

Components deemed unfit for use shall be disposed of securely to prevent potential reuse or unauthorized access to sensitive data.

Review and Updates

This Policy shall be reviewed at least annually by the Information Security team and Management to assess its effectiveness, identify areas for improvement, and ensure alignment with changing security needs and regulatory requirements. Updates shall be made as necessary to maintain a robust and secure environment for the organization's information systems and assets.

Compliance

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Change	Responsible	Summary of Change
September 2023	DOA/ITMD	Draft Created.