Supply Chain Risk Management Policy

Date Issued: 06/11/2026
Revised Date: 06/11/2026
Authority: Chief Information Security Officer

Policy Statement

The purpose of this policy is to establish the State of Minnesota's supply chain risk management program. This program ensures that relationships with vendors, contractors, and suppliers are managed to identify, assess, and mitigate risks that could impact the State's mission-critical assets, functions, and services.

Violations of this policy by state agency employees will be subject to discipline, up to and including discharge. Violations of this policy by third parties will be subject to appropriate action.

In cases where non-compliance involves unlawful activity, individuals may also be subject to civil or criminal penalties under applicable federal or state laws.

Scope of Policy

This policy applies to:

1. All departments, agencies, offices, councils, boards, commissions, and other entities listed as in scope for IT consolidation and IT oversight in the Information Security and Risk Management Applicability Standard.
2. All vendors, contractors, and suppliers that provide goods and services to in-scope State entities.

Reason for the policy

The reason for this policy is for the State of Minnesota to address the risks associated with the products, services, and solutions bought, used, and offered to its constituents. These risks are unique in how they can potentially undermine the operation of State functions and must be addressed by both the State and the vendor, contractor, or supplier to prevent such an incident.

Roles & Responsibilities

1. Employees, Vendors, and Contractors are responsible for:
   1.1. Reading, understanding, and applying relevant supply chain risk management policies, standards, and procedures.

1.2. Ensure supply chain risk management is incorporated into project planning, vendor solicitation, procurement, system integration, and vendor management processes prior to submitting a requisition request.
1.3. Ensure that vendors and contractors follow required supply chain risk management controls.
1.4. Contact appropriate management personnel with questions about risk management policies, standards, or procedures.

2. Project Managers, Product Owners, and Business Analysts are responsible for:
   2.1. Ensure all project scoping and project work complies with all MNIT policies, standards, and procedures.
   2.2. Report third-party assessment results to leadership to help inform risk posture.
   2.3. Communicating to procurement when a potential purchase may be in scope for supply chain risk management
3. Supervisors and Managers are responsible for:
   3.1. Ensure employees and contractors are proficient in supply chain risk management policies, standards, and procedures that are relevant to their roles.
   3.2. Ensuring that the policy is implemented and enforced for all third-party engagements.
   3.3. Hold employees accountable for following supply chain risk management policies, standards, and procedures.
   3.4. Ensuring that KPIs are measured, monitored, and reported to the CISO on a quarterly/annual basis.
4. Procurement Personnel are responsible for:
   4.1. Ensure all in-scope supplier agreements include terms related to supply chain risk management including security controls and reporting obligations.
5. Information Technology Personnel are responsible for:
   5.1. Apply appropriate supply chain risk controls during the design, operation, and maintenance of systems and services.
   5.2. Work with third parties to ensure security controls are implemented for critical systems and components.
6. Information Security Personnel are responsible for:
   6.1. Ensure supply chain security requirements are aligned with organizational security policies.
   6.2. Review and update supply chain risk management solicitation and contract language as needed.
   6.3. Monitor supply chain risks and respond to any security breaches or incidents.
   6.4. Implement a comprehensive supply chain risk management program that includes risk identification, mitigation, and monitoring.
7. Governance, Risk, and Compliance Personnel are responsible for:
   7.1. Develop, maintain, and assess compliance with this policy.
   7.2. Maintain this policy to be consistent with applicable federal and state laws, executive orders, directives, regulations, and MNIT policies.
   7.3. Provide training on supply chain risk management policies, standards, and procedures.
   7.4. Assist with the interpretation and application of this policy.
   7.5. Coordinate with Legal and Agency Data Practices personnel to validate alignment.
8. State Chief Information Security Officer (CISO) and/or designee is accountable for:
   8.1. Review and approve this policy.
   8.2. Manage supply chain incidents.
   8.3. Design and implement State of Minnesota supply chain strategy.
   8.4. Management of overall State of Minnesota supply chain security-related risk.

Related Information

Supply Chain Risk Management Standard

Authority and Compliance

Laws, executive orders, directives, regulations, policies, standards, and guidelines that govern the Supply Chain Risk Management Policy execution.

1. **Policies**
    a. Information Security Risk Management Program Policy
    b. Secure Systems Development and Acquisition Policy
    c. Criminal Justice Information Services (CJIS) Security Policy
2. **Legislation**
    a. Internal Revenue Code § 6103
    b. Minnesota Statues Chapter 13: Government Data Practices
    c. Minnesota Statutes Chapter 16C: State Procurement (2024) – Key sections: § 16C.03 (Procurement Duties)
3. **Guidelines**
    a. IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies
    b. GovRAMP Standards
    c. NIST SP800-53, Revision 5
    d. NIST SP800-161, Revision 1
    e. NIST SP800-60, Volume II, Revision 1

Definitions

Table 1: Definitions

Term	Definition
Third-party vendor	Any type of vendor that is an external entity providing goods/services, that may or may not have a direct contract.
Contractor	A third party with a formal contract to deliver specific work.
Covered articles	Information technology, including cloud computing services of all types; telecommunications equipment or telecommunications services; the processing of information on a federal or non-federal information system, subject to the requirements of the Data Protection Categorization Standard; and all Internet of Things / Operational Technology (e.g., hardware, systems, devices, software, or services that include embedded or incidental information technology).
Risk owner	A person or entity with the accountability and authority to manage a risk.

History

Table 2: Version History

Version	Description	Date
1.0	Initial version reviewed and approved executive leadership	6/11/2026

Contact

grc@state.mn.us