Threat and Vulnerability Management Policy

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.6
Effective Date: 1/1/2016
Revised: 10/1/2023
Approved: John Israel, State Chief Information Security Officer **Date:** 1/31/2024

Policy Statement

The State of Minnesota must maintain a threat and vulnerability management program to identify and remediate information security vulnerabilities.

Reason for the policy

To adequately protect the data and services entrusted to the State of Minnesota by the public it is necessary to identify and remediate vulnerabilities within State IT systems. Monitoring for threats, vulnerabilities, and advisories along with vulnerability scanning and penetration testing identify security weaknesses within systems and allows for prioritization of resources to address the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of State data.

Roles & Responsibilities

- Employees, Vendors, and Contractors
  - Be aware of and follow relevant information security policies, standards, and procedures.
  - Ensure information security is incorporated into processes and procedures.
  - Ensure contract language with contractors and vendors includes required information security controls.
  - Consult with information security staff on the purchase and procurement of information technology systems or services.
  - Contact information security staff or email GRC@state.mn.us with questions about the information security policies, standards, or procedures.
- Supervisors and Managers

    - Ensure employees and contractors are proficient in the information security policies, standards and procedures that are relevant to their role.
    - Hold employees accountable for following the information security policies, standards, and procedures.
- Information Technology Personnel
    - Apply appropriate controls to the design, operation and maintenance of systems, processes, and procedures in conformance with the information security policies, standards, and procedures.
- Information Security Personnel
    - Develop, maintain, and assess compliance with the information security policies, standards, and procedures.
    - Develop, maintain, and implement a comprehensive information security program.
    - Provide training on information security policies, standards, and procedures.
    - Assist agencies and personnel with understanding and implementing information security policies, standards, and procedures.
    - Notify appropriate personnel of applicable threats, vulnerabilities and risks to State data or systems.
- Agency Data Practices Personnel

    - Assist agencies and personnel with questions on proper data use, collection, storage, destruction, and disclosure.

Applicability

This policy applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government.

Related Information

Threat and Vulnerability Management Standard

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Version	Description	Date
1.0	Initial Release	4/21/2015

Version	Description	Date
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date and Template	12/20/2016
1.3	Updated Compliance Enforcement Date	10/4/2017
1.4	Modified document title and minor edits	3/10/2020
1.5	Removed Compliance Enforcement Date and grammatical updates	10/1/2022
1.6	Updated version number and revision date	10/1/2023

Contact

GRC@state.mn.us