

Security Monitoring and Response Policy

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

Version: 1.7

Effective Date: 1/1/2016

Revised: 12/31/2024

Approved: John Israel, State Chief Information Security Officer **Date:** 3/20/2025

Policy Statement

The State must implement information security logging, monitoring, and incident management controls to ensure the effective detection, response and handling of information security events or incidents that could affect the confidentiality, integrity or availability of State data or system.

Employees must abide by the terms of this policy. Employees who violate this policy may be subject to discipline, up to and including discharge.

Reason for the Policy

Implementing security monitoring and incident response controls ensures the effective detection, response and handling of security events and incidents that affect the availability, integrity, and confidentiality 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

Logging and Monitoring Standard

Security Incident Management Standard

State Standards and Authoritative Source Cross Mapping

History

Table 1. Version History

Version	Description	Date
1.0	Initial Release	7/8/2015
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 and Template	10/17/2017
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 revised date	10/1/2023
1.7	Added enforcement language; updated version and revision date	12/2/2024

Contact

GRC@state.mn.us