Information Security Risk Management Standard

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

Version:	1.8	
Effective Date:	1/1/2016	
Revised:	12/31/2024	
Approved:	John Israel, State Chief Information Security Officer	**Date:** 3/20/2025

Standard Statement

To ensure State of Minnesota's leadership makes informed decisions about the protection of systems and data, a formal and robust information security risk management program must be developed and maintained. This standard sets the baseline requirements to assess risks to State data, track and monitor control gaps, and provide leadership reports on information security risks to the State.

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

Table 1 - Information Security Risk Management Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Information Security Risk Management Program	Establish and maintain an enterprise information security risk management program to manage risks to State data, systems, and operations. The program must include processes for ensuring that plans for conducting security testing, training, and monitoring activities: • Are developed and maintained. • Continue to be executed in a timely manner. • Are consistent with the risk management strategy and priorities. This program must be reviewed and updated at least every two years or as needed to address changes in business processes.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
2	Information Security Risk Assessment	An information security risk assessment must be performed on all new and significantly changed systems, processes, and third-party vendors and contractors with access to State data or systems. This requirement includes proof of concept and proof of value engagements. This assessment must: • Include an assessment of the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the system, process, or third party and the information it processes, stores, or transmits. • Document risk assessment results in a risk assessment report.. • Be updated upon any significant changes to the system's environment or threat landscape. • Be updated at least every 3 years for all systems and processes with data protection categorization of High. Third parties supplying services must be assessed annually. • Identify critical assets, threats, and vulnerabilities. • Identify the likelihood and impact of the risks. • Communicate risks to agency and security leadership. Agency leadership is responsible for prioritizing and addressing risks identified in the risk assessment. Risk Assessment reports must be maintained for at least 6 years.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
3	Security Assessments	A security assessment must be performed on systems, processes, and physical locations at least annually and upon significant changes. This assessment must: • Follow a documented security assessment plan including assessment procedures to be used to determine control effectiveness. • Assess compliance with State enterprise security policies and standards. • Assess compliance with any applicable regulations. • Be completed by qualified internal or external assessors. • Assign findings a risk rating based on likelihood and impact. • Produce a security assessment report that documents the results of the assessment. • Provide the results of the security control assessment to key agency and IT stakeholders. All or portions of an assessment that is performed for other purposes may be used to address this requirement for the systems and controls tested if: • The State Chief Information Security Officer (CISO) or delegate approves. • The assessment is performed by qualified independent assessors. • The controls are validated to be at least as strong as the State policies and standards requirements. Security Assessment reports must be maintained for at least 6 years.	High
4	Vendor Security Assessments	The security practices and compliance with any applicable regulations of third parties with access to State data or systems must be reviewed prior to beginning the engagement with the third party and at least annually. This requirement includes proof of concept and proof of value engagements. Vendor Assessment reports must be maintained for at least 6 years.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
5	Remediation Plan	All identified information security risks, findings, weaknesses, and deficiencies must have a documented remediation plan in place within 30 days of identification that: • Outlines the actions that will be taken to remediate the risk. • Includes milestones and timelines including anticipated remediation date. • Is updated at least monthly to reflect changes in remediation status, approach, and risks to the environment. All findings and remediation plans must be documented in a centralized findings management tool to help ensure that the remediation plans are accurate, up to date, and readily available.	Low Moderate High
6	Information Security Risk Monitoring and Reporting	An information security risk monitoring and reporting program must be in place to: • Monitor the status of known findings, exceptions, and vulnerabilities at least monthly. • Provide agency, technical and security leadership relevant and current metrics outlining the risks to State data at least quarterly. • Track remediation efforts and respond to findings, exceptions, and vulnerabilities that are not on track to be resolved in the appropriate timeframes. • Correlate findings, exceptions, and vulnerabilities to determine the cumulative risks to assets.	Low Moderate High

Reason for the Standard

This standard ensures that information security risks to State data are identified and addressed in a timely manner and that leadership has the information needed to make informed, risk-based decisions.

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

Related Information

Information Security and Risk Management Program Policy

Data Protection Categorization Standard

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 2. Version History

Version	Description	Date
1.0	Initial Release	4/21/2015
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date	12/20/2016
1.3	Updated Compliance Enforcement Date	10/22/2017
1.4	Scheduled Document Update	3/10/2020
1.5	Scheduled Document Refresh	11/1/2021
1.6	Modified vendor security assessment requirements	10/1/2022
1.7	Clarified requirements for PoC and PoV; updated version number and revision date	10/1/2023
1.8	Added enforcement language; updated version and revision date	12/2/2024

Contact

GRC@state.mn.us