MINNESOTA
IT SERVICES

# Information Security Program 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 the State of Minnesota is adequately managing information security across the enterprise, a comprehensive information security program under the leadership of the State Chief Information Security Officer (CISO) must be developed and maintained. Through this program the State CISO is authorized to set information security policies and standards, identify, track and report on security risks to State systems and data, and monitor for and address security related incidents.

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 Program Controls

| Control Number | Control Name | Control Detail | Applicable Data Protection Categorization |
|---|---|---|---|
| **1** | Information Security Program | The State will maintain a comprehensive information security program with dedicated resources under the leadership of the State Chief Information Security Officer. | Low<br>Moderate<br>High |

| Control Number | Control Name | Control Detail | Applicable Data Protection Categorization |
|---|---|---|---|
| **2** | Information Security Program Plan | An enterprise-wide information security program plan must be established and maintained that:<br>• Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.<br>• Determines information protection needs arising from the defined mission/business processes, and revises the processes, as necessary, until it defines achievable protection needs.<br>• Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.<br>• Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.<br>• Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical).<br>• Is approved by a senior official with responsibility and accountability for the risk incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.<br>• Is reviewed and updated at least annually to address organizational changes and problems identified during plan implementation or security control assessments.<br>• Is protected from unauthorized disclosure and modification | Low<br>Moderate<br>High |

| Control Number | Control Name | Control Detail | Applicable Data Protection Categorization |
|---|---|---|---|
| **3** | Information Security Workforce | The information security workforce must have sufficient knowledge, experience, and training to effectively execute their roles. An information security workforce development and improvement program must be in place. | Low<br>Moderate<br>High |
| **4** | Information Security Policies and Standards | A comprehensive set of information security policies and standards must be developed, documented, approved, and made available to all impacted State personnel. The information security policies and standards must address information security risks to the State, legal and regulatory obligations and agency needs. The State CISO or delegate must approve any exceptions to the policies and standards. | Low<br>Moderate<br>High |
| **5** | Information Security Policies and Standards Updates | Information security policies and standards must be reviewed on an annual basis and updated to address changes in agency objectives, legal and regulatory obligations, and information security risks. Copies of policies and standards must be maintained for at least 6 years following their publication for historical reference. | Low<br>Moderate<br>High |
| **6** | Information Security Metrics and Reporting | Information security program performance metrics must be provided to agency, security, and IT leadership at least quarterly. | Low<br>Moderate<br>High |
| **7** | Information Sharing | The State information security program will participate in the local and national information security community to facilitate ongoing security awareness and training and stay current with security best practices. The State will also promptly share relevant, timely and actionable classified and unclassified security information according to standard procedures and protocols with federal, local and private partners with appropriate classifications. | Low<br>Moderate<br>High |

| Control Number | Control Name | Control Detail | Applicable Data Protection Categorization |
|---|---|---|---|
| **8** | Operational Procedures | Processes and procedures that implement the enterprise information security policies and standards must be developed and maintained. Procedures must be reviewed at least annually. Copies of operational procedures must be maintained for at least 6 years following their publication for historical reference. | Low<br>Moderate<br>High |
| **9** | Insider Threat Program | A comprehensive insider threat program must be implemented that:<br>• Includes a cross-discipline, insider threat incident-handling team.<br>• Provides insider threat policies and implementation plans.<br>• Conducts host-based user monitoring of individual employee activities.<br>• Provides insider threat awareness training to employees.<br>• Receives access to information from all offices within the organization (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis.<br>• Conducts self-assessments of organizational insider threat posture. | Low<br>Moderate<br>High |

## Reason for the Standard

This standard ensures that roles and responsibilities for information security within the State of Minnesota are assigned. It also ensures that information security policies and standards, are in place and designed to address State of Minnesota compliance obligations and business needs.

## 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

Information Security Risk Management 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 Refresh | 3/10/2020 |
| 1.5 | Scheduled Document Refresh | 11/1/2021 |
| 1.6 | Scheduled document refresh | 10/1/2022 |
| 1.7 | 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