Physical and Environmental Security 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

Physical access to State systems, media, and data must be controlled to ensure the confidentiality, availability, and integrity of State data.

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. Physical and Environmental Security Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Labeling	Media must be labeled to indicate the handling and access requirements.	High
2	Secure Storage of Paper and Electronic Media	Paper and electronic media containing State data must be kept under the immediate protection and control of authorized personnel or securely locked up.	High
3	Media Inventory	Electronic media containing State data must be inventoried at least annually. Inventories must be documented and any discrepancies with previous inventories must be investigated and communicated to the security incident response team.	High
4	Offsite Storage	All media sent to an off-site storage location must be: • Labeled • Encrypted. • Secured in a locked container with the key retained in State control. • Protected from unauthorized access. Off-site storage locations must be secure, and the security of the storage location must be assessed annually.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

5	Media Transport	The transport of any kind of paper or electronic media containing State data must be strictly controlled, including the following:
		• Categorize the media based on the data it contains.
		• Send the media by secured courier or other secure delivery method that can be accurately tracked.
		• Monitor the transport to ensure that each shipment is properly and timely received and acknowledged.
		• Document the transport of all media. Documentation must contain:
		  ○ a. The name of media recipient.
		  ○ b. Signature of media recipient.
		  ○ c. Date/time media received.
		  ○ d. Media control number and contents.
		  ○ e. Movement or routing information.
		  ○ f. If disposed of, the date, time, and method of destruction.
		• Ensure only authorized personnel approve all media that is moved from a secured area including when media is distributed to individuals.
		• Restrict the activities associated with the transport of media to authorized personnel.
		• Maintain accountability for media during transport outside of secured areas.
		• Encrypt all electronic media containing data with data protection categorization of High.
		• Ensure a current, retrievable copy of data is available for systems containing data with a Data Protection Categorization of High before movement of servers.
		• Paper or electronic media containing Federal Tax Information (FTI) must be double sealed using one of the following:
		  ○ One envelope within another envelope with the inner envelope marked “confidential” with some indication that only the designated official or delegate is authorized to open it.
		• Boxes sealed with tamper evident seals.
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
6	Secure Disposal of Paper	Paper containing State data must be securely disposed of when no longer needed for business or legal reasons and in accordance with record retention requirements by: • Ensuring all employees have access to and use secure shred bins or crosscut shredding devices. ○ These devices must be crosscut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size or smaller. • Physically securing shred bins. • Emptying secure shred bins on a periodic basis to ensure they do not fill up. • Shredding, incinerating, or pulping hard-copy materials so that State data cannot be reconstructed. • Ensuring the disposal or destruction is witnessed or carried out by authorized personnel. • Third parties performing disposal must be National Association for Information Destruction (NAID) certified and the state must maintain a copy of, and periodically validate the NAID certification.	Moderate High

7	Secure Disposal of Electronic Media	Media must be securely disposed of when it is no longer needed for business or legal reasons and in accordance with record retention requirements as follows:
		• Review and approve media to be sanitized to ensure compliance with business, legal, and records retention requirements.
		• Sanitize or destroy all media prior to disposal, release out of State control or reuse following the NIST Special Publication 800-88 Revision 1 Sanitization Methods
		  ○ Media that will be reused in the same environment with the same or higher data protection categorization can follow the "Clear" method.
		  ○ Media that will be surplused, returned to the vendor or otherwise sent outside of state control, or reused in an environment with a lower Data protection categorization must follow the "Purge" or "Destroy" methods.
		  ○ Nonfunctional media, media that cannot be "Purged", and media not being reused must follow the "Destroy" method.
		• Ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
		• Verify the media sanitization or destruction was successful by testing a representative sample at least once per year (every 365 days).
		• Document sanitization and destruction actions including:
		  ○ Personnel who reviewed and approved sanitization or disposal actions.
		  ○ Types of media sanitized.
		  ○ Sanitization methods used.
		  ○ Date and time of the sanitization actions.
		  ○ Personnel who performed the sanitization.
		  ○ Verification actions taken.
		  ○ Personnel who performed the verification.
		  ○ Disposal action taken.
		• Provide the business a certificate of destruction confirming disposition of the media.
		
		Third parties performing data disposal must be National Association for Information Destruction (NAID) certified and the state must maintain a copy of, and periodically validate the NAID certification.
			Moderate
			
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
8	Physical Barriers	Areas of the facility containing State systems and data must be physically separated from other areas of the facility by: • Separating nonpublic areas from public areas with physical barriers (e.g., walls, doors, turnstiles, etc.) and identifying areas as nonpublic with prominent postings. • Separating sensitive areas such as data centers, network closets, and areas storing or processing data with data protection categorization of High from other areas of the facility using at least two physical barriers. Protected information must be containerized in areas where other than authorized employees may have access afterhours. • Minimizing the number of entrances to nonpublic and sensitive areas. • Controlling entry and exit points to nonpublic and sensitive areas of the facility using physical access control systems/devices and/or guards. Restricting physical access to wireless access points, gateways, VoIP network hardware, handheld devices, networking/communications hardware, and telecommunication lines.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

9	Physical Access Control	Physical access to nonpublic and sensitive areas (data centers, wiring closets, rooms where data with a Data Protection Categorization of High is stored or processed, etc.) must be controlled by:
		• Developing, approving, and maintaining a list of individuals with authorized access to nonpublic and sensitive areas of the facility. This list must include:
		  ○ Name of individual.
		  ○ Agency or department name.
		  ○ Name and contact information of agency point of contact.
		  ○ Purpose for access.
		• Reviewing and updating the access list detailing authorized access by individuals at least every six months for data centers and at least annually for all other areas.
		• Authorizing access to nonpublic and sensitive areas based on the individual's job function.
		• Prohibiting "piggybacking" or "tailgating" into nonpublic or sensitive locations.
		• Verifying individual access authorizations before granting access.
		• Enforcing physical access authorizations at defined entry/exit points
		• Issuing badge access, keys and/or combinations only to authorized individuals.
		• Revoking access when no longer needed and ensuring all physical access mechanisms, such as keys, access cards, etc., are returned, changed and/or disabled.
		• Requiring the use of two factor authentication for physical access to data centers.
		• Requiring the inspection of all bags and items entering data centers and limiting access to only those items that are needed to perform work.
		• Requiring the completion of required background checks and training prior to granting access to data centers.
			Low
			Moderate
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

10	Physical Access Monitoring	Video cameras and/or access control systems (e.g., badge readers, smart cards, biometrics, etc.) must be used to monitor and track all physical access attempts to nonpublic and sensitive areas. Video and/or access control logs must:
		• Capture the following information:
		  ○ The owner of the access control device requesting access and/or the identity of the individual requesting access.
		  ○ The success or failure of the request.
		  ○ The date and time of the request.
		• Be reviewed at least weekly and upon occurrence of security incidents involving physical security and correlated with other entries.
		• Unauthorized access must be reported to the security incident response team for investigation.
		• Stored for at least 90 days for data centers and areas containing data with a data protection categorization of High.
		• Be monitored 24 hours per day, 7 days per week by trained personnel who respond to potential incidents.
		• Be analyzed by automated mechanisms to recognize potential intrusions and initiate designated response actions.
			Moderate
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
11	Tamper Prevention	Systems processing credit cards or located in public spaces and all video cameras and physical access control devices regardless of physical location, must be: • Protected from unauthorized modification or substitution. • Periodically inspected to detect tampering or unauthorized substitution. Users of these systems must be trained to detect tampering. Training should instruct users to: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Low Moderate High
12	Output Device Locations	Prevent the unauthorized viewing of State data by: • Locating printers and fax machines in secure areas. • Using privacy screens and/or positioning monitors and laptop screens so that unauthorized users cannot view the screen.	High
13	System Locations	Systems must be positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Low Moderate High
14	Physical Device Lock	Workstations and laptop computers containing Federal Tax Information (FTI) must be physically secured to large objects such as desks or tables when not in use. Smaller equipment such as smartphones and tablets must be locked in a filing cabinet or desk drawer when not in use.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
15	Alternate Work Locations	Personnel working from locations not controlled by the State must ensure the protection of State data. Appropriate security controls must be implemented at alternate work sites that include, but are not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites. Personnel must be provided a means to communicate with information security personnel in case of security incidents or problems. Telework locations for personnel accessing Federal Tax Information must be inspected to ensure that this data is adequately protected. The results of each inspection must be fully documented.	High
16	Physical Access Device Management	Keys, combinations, and other physical access devices must be protected by: • Storing keys, combinations, and other physical access devices in a secure location. • Inventorying and reconciling all keys and other physical access devices at least annually. • Changing combinations at least annually and when an employee who knows or has access to them no longer has a need to access the area, room, or container. • Only giving keys, combinations, and other physical access devices to those who have a frequent need to have access to the area, room or container. • Prohibiting the writing of combinations or PINs on a sticky-note, calendar pad, or any other item (even though it is carried on one's person or hidden from view). If needed a written copy of the combination may be kept in an envelope that is secured in a container with appropriate security controls.	Moderate High
17	Delivery and Removal	All systems being brought into or removed from State data centers must be authorized, monitored, controlled, and documented.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
18	Personnel Badges	State personnel with access to nonpublic areas of State facilities must be assigned a photo ID badge that distinguishes State personnel from visitors. Badges must be always worn above the waist and visible while inside nonpublic areas.	Low Moderate High

19	Visitor Access	Visitors to nonpublic or sensitive areas must be:
		• Authorized before entering.
		• Escorted and always monitored within nonpublic or sensitive areas.
		• Identified by examining government issued photo identification (e.g., state driver's license or passport) for data centers and areas containing Federal Tax Information.
		• Given a badge or other identification that:
		  ○ Expires no later than the end of the visit.
		  ○ Visibly distinguishes the visitors from authorized personnel.
		  ○ Is returned before leaving the facility or at the date of expiration.
			Low
			Moderate
			High

20	Visitor Log	A visitor log must be used to maintain a physical audit trail of all visitor activity to nonpublic and sensitive areas. This visitor log must:
		• Be retained for a minimum of 5 years.
		• Be closed out at the end of each month and reviewed by management.
		• Contain the following information:
		  ○ Name of the visitor.
		  ○ Organization of the visitor.
		  ○ Signature of the visitor (electronic or physical).
		  ○ Form of identification reviewed (if required).
		  ○ Date of access.
		  ○ Time of entry and departure.
		  ○ Purpose of visit.
		  ○ Name and organization of authorized escort.
			Low
			Moderate
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

21	Maintenance Personnel Access	Physical access for cleaning, security and maintenance personnel must controlled by:
		• Maintaining a list of authorized maintenance organizations or personnel. This list must be updated at least monthly and include:
		  ○ Name of vendor/contractor.
		  ○ Name and phone number of State point of contact authorizing access.
		  ○ Name and contact information of vendor point of contact.
		  ○ Address of vendor/contractor.
		  ○ Purpose and level of access.
		• Ensuring that non-escorted maintenance and cleaning personnel have completed the same training, screening, and approval as authorized employees.
		• Designating State personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not have the required access authorizations.
			Low
			Moderate
			High

22	Facilities Maintenance	Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets. Repairs and modifications to the physical components of a facility which are related to security (for example, door hinges and handles, walls, doors, and locks) must be approved and documented.	Moderate High
23	Power Equipment and Cabling	Data center power equipment and power cabling for systems in the data center must be protected from damage and destruction.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
24	Emergency Shutoff	Data centers must have the capability of shutting off power to the data center or individual systems in emergency situations. Emergency shutoff switches or devices must be: • Located where they can safely and easily be accessed. • Protected from unauthorized or unintended activation.	Low Moderate High
25	Emergency Power	Data centers must have: • A short-term uninterruptible power supply in place to facilitate the transition of systems to long-term alternate power in the event of a primary power source loss. • A long-term alternate power supply that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	Low Moderate High
26	Emergency Lighting	Automatic emergency lighting that activates in the event of a power outage or disruption must be maintained and in place to cover: • All emergency exits and evacuation routes within the facility. • All areas within the facility supporting essential missions and business functions.	Low Moderate High
27	Fire Protection	Fire suppression and detection devices/systems must be in place that: • Are supported by an independent energy source. • Activate automatically. • Notify facilities personnel and the local fire department in the event of a fire detection or suppression activation.	Low Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

28	Temperature and Humidity Controls	Data centers must have controls in place to:
		• Maintain temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels.
		• Monitor temperature and humidity levels. Alert appropriate personnel in the event the temperature or humidity fall outside of acceptable levels
		  ○ Evaluate the level of alert and follow prescribed guidelines for that alert level.
		  ○ Alert component management of possible loss of service and/or media.
		  ○ Report damage and provide remedial action. Implement contingency plan, if necessary.
			Low
			Moderate
			High

29	Water Damage Protection	Data centers must have controls in place to prevent damage from water leakage by: • Providing master shutoff or isolation valves that are accessible, working properly and known to data center facilities personnel. • Using automated mechanisms to detect the presence of water in the data center and alert data center facilities personnel.	Low Moderate High

Reason for the Standard

Physical security is essential to ensure the confidentiality availability and integrity of State data. Physical controls prevent the unauthorized or unintended disclosure or destruction 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 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

Physical and Environmental Security Policy

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 2. 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	10/26/2017
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	Table formatting; 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