



Information Technology for Minnesota Government

# ENTERPRISE PHYSICAL AND ENVIRONMENTAL SECURITY STANDARD

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

**Version:** 1.1  
**Effective Date:** 1/1/2016  
**Compliance Enforcement Date:** 1/1/2017  
**Approval:** Signature on file

## Standard Statement

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

### *Physical and Environmental Security Controls*

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
1	Labeling	Systems and 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 an 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 electronic media sent to an off-site storage location must be: <ul style="list-style-type: none"><li>• Encrypted.</li><li>• Locked in a turtle case with the key retained in State control.</li></ul>	High

<p>5</p>	<p>Media Transport</p>	<p>The transport of any kind of paper or electronic media containing State data must be strictly controlled, including the following:</p> <ul style="list-style-type: none"> <li>• Categorize the media based on the data it contains.</li> <li>• Send the media by secured courier or other secure delivery method that can be accurately tracked.</li> <li>• Monitor the transport to ensure that each shipment is properly and timely received and acknowledged.</li> <li>• Document the transport of all media.</li> <li>• Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).</li> <li>• Restrict the activities associated with the transport of media to authorized personnel.</li> <li>• Maintain accountability for media during transport outside of secured areas.</li> <li>• All electronic media containing data with data protection categorization of High must be encrypted.</li> <li>• Paper or electronic media must be double-sealed using one of the following:                         <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ Boxes sealed with tamper evident seals.</li> </ul> </li> </ul>	<p>High</p>
<p>6</p>	<p>Secure Disposal of Paper</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Ensuring all employees have access to and use secure shred bins or crosscut shredding devices.</li> <li>• Physically securing shred bins.</li> <li>• Emptying secure shred bins on a periodic basis to ensure they do not fill up.</li> <li>• Shredding, incinerating or pulping hard-copy materials so that State data cannot be reconstructed.</li> <li>• Ensuring the disposal or destruction is witnessed or carried out by authorized personnel.</li> </ul>	<p>Moderate High</p>
<p>7</p>	<p>Secure Disposal of Electronic Media</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Review and approve media to be sanitized to ensure compliance with business, legal, and records retention requirements.</li> </ul>	<p>Moderate High</p>

		<ul style="list-style-type: none"> <li>• Sanitize or destroy all media prior to disposal, release out of State control or reuse.</li> <li>• Ensure the sanitization or destruction is witnessed or carried out by authorized personnel.</li> <li>• Verify the media sanitization or destruction was successful.</li> <li>• Document sanitization and destruction actions including:             <ul style="list-style-type: none"> <li>○ Personnel who reviewed and approved sanitization or disposal actions.</li> <li>○ Types of media sanitized.</li> <li>○ Sanitization methods used.</li> <li>○ Date and time of the sanitization actions.</li> <li>○ Personnel who performed the sanitization.</li> <li>○ Verification actions taken.</li> <li>○ Personnel who performed the verification.</li> <li>○ Disposal action taken.</li> </ul> </li> <li>• Provide the business a certificate of destruction confirming disposition of the media.</li> </ul>	
<p style="text-align: center;"><b>8</b></p>	<p style="text-align: center;">Physical Barriers</p>	<p>Areas of the facility containing State systems and data must be physically separated from other areas of the facility by:</p> <ul style="list-style-type: none"> <li>• Separating nonpublic areas from public areas with physical barriers (e.g., walls, doors, turnstiles, etc.) and identifying areas as nonpublic with prominent postings.</li> <li>• 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 physical barriers.</li> <li>• Minimizing the number of entrances to nonpublic and sensitive areas.</li> <li>• Controlling entry and exit points to nonpublic and sensitive areas of the facility using physical access control systems/devices and/or guards.</li> <li>• Restricting physical access to wireless access points, gateways, handheld devices, networking/communications hardware and telecommunication lines.</li> </ul>	<p style="text-align: center;">Low Moderate High</p>
<p style="text-align: center;"><b>9</b></p>	<p style="text-align: center;">Physical Access Control</p>	<p>Physical access to nonpublic and sensitive areas must be controlled by:</p> <ul style="list-style-type: none"> <li>• Developing, approving and maintaining a list of individuals with authorized access to nonpublic and sensitive areas of the facility. This list must include:             <ul style="list-style-type: none"> <li>○ Name of individual.</li> <li>○ Agency or department name.</li> <li>○ Name and contact information of agency point of contact.</li> </ul> </li> </ul>	<p style="text-align: center;">Low Moderate High</p>

		<ul style="list-style-type: none"> <li>○ Purpose for access.</li> <li>● 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.</li> <li>● Authorizing access to nonpublic and sensitive areas based on the individual’s job function.</li> <li>● Prohibiting “piggybacking” or “tailgating” into nonpublic or sensitive locations.</li> <li>● Issuing badge access, keys and/or combinations only to authorized individuals.</li> <li>● Revoking access when no longer needed and ensuring all physical access mechanisms, such as keys, access cards, etc., are returned, changed and/or disabled.</li> <li>● Requiring the use of two factor of authentication for physical access to data centers.</li> <li>● Requiring the inspection of all bags and items entering data centers and limiting access to only those items that are needed to perform work.</li> <li>● Requiring the completion of required background checks and training prior to granting access to data centers.</li> </ul>	
10	Physical Access Monitoring	<p>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:</p> <ul style="list-style-type: none"> <li>● Capture the following information:                             <ul style="list-style-type: none"> <li>○ The owner of the access control device requesting access and/or the identity of the individual requesting access.</li> <li>○ The success or failure of the request.</li> <li>○ The date and time of the request.</li> </ul> </li> <li>● Be reviewed at least monthly and correlated with other entries.</li> <li>● Unauthorized access must be reported to the security incident response team for investigation.</li> <li>● Stored for at least 90 days for data centers and areas containing data with a data protection categorization of High.</li> <li>● Be monitored 24 hours per day, 7 days per week by trained personnel who respond to potential incidents.</li> <li>● Be analyzed by automated mechanisms to recognize potential intrusions and initiate designated response actions.</li> </ul>	Moderate High
11	Tamper	Systems located in public spaces and all video cameras and	Low

	Prevention	physical access control devices regardless of physical location, must be: <ul style="list-style-type: none"> <li>Protected from unauthorized modification or substitution.</li> <li>Periodically inspected to detect tampering or unauthorized substitution.</li> </ul>	Moderate High
12	Output Device Locations	Prevent the unauthorized viewing of State data by: <ul style="list-style-type: none"> <li>Locating printers and fax machines in secure areas.</li> <li>Using privacy screens and/or positioning monitors and laptop screens so that unauthorized users cannot view the screen.</li> </ul>	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
15	Alternate Work Locations	Personnel working from locations not controlled by the State must ensure the protection of State data.  Telework locations for personnel accessing Federal Tax Information must be inspected at least twice per year to ensure that this data is adequately protected. The results of each inspection must be fully documented.	Moderate High
16	Physical Access Device Management	Keys, combinations and other physical access devices must be protected by: <ul style="list-style-type: none"> <li>Storing keys, combinations and other physical access devices in a secure location.</li> <li>Inventorizing and reconciling all keys and other physical access devices at least annually.</li> <li>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.</li> <li>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.</li> </ul>	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
18	Personnel Badges	State personnel with access to nonpublic areas of State facilities must be assigned a badge that distinguishes State personnel from visitors. Badges must be worn and visible at all times while inside nonpublic areas.	Low Moderate High
19	Visitor Access	<p>Visitors to nonpublic or sensitive areas must be:</p> <ul style="list-style-type: none"> <li>• Authorized before entering.</li> <li>• Escorted and monitored at all times within nonpublic or sensitive areas.</li> <li>• Identified by examining government issued photo identification (e.g., state driver's license or passport) for data centers and areas containing Federal Tax Information.</li> <li>• Given a badge or other identification that: <ul style="list-style-type: none"> <li>○ Expires no later than the end of the visit.</li> <li>○ Visibly distinguishes the visitors from authorized personnel.</li> <li>○ Is returned before leaving the facility or at the date of expiration.</li> </ul> </li> </ul>	Low Moderate High
20	Visitor Log	<p>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:</p> <ul style="list-style-type: none"> <li>• Be retained for a minimum of 12 months.</li> <li>• Be closed out at the end of each month and reviewed by management.</li> <li>• Contain the following information: <ul style="list-style-type: none"> <li>○ Name of the visitor.</li> <li>○ Organization of the visitor.</li> <li>○ Signature of the visitor (electronic or physical).</li> <li>○ Form of identification reviewed (if required).</li> <li>○ Date of access.</li> <li>○ Time of entry and departure.</li> <li>○ Purpose of visit.</li> <li>○ Name and organization of authorized escort.</li> </ul> </li> </ul>	Low Moderate High
21	Maintenance Personnel Access	<p>Physical access for cleaning, security and maintenance personnel must controlled by:</p> <ul style="list-style-type: none"> <li>• Maintaining a list of authorized maintenance organizations or personnel. This list must be updated at least every 6</li> </ul>	Low Moderate High

		<p>months and include:</p> <ul style="list-style-type: none"> <li>○ Name of vendor/contractor.</li> <li>○ Name and phone number of State point of contact authorizing access.</li> <li>○ Name and contact information of vendor point of contact.</li> <li>○ Address of vendor/contractor.</li> <li>○ Purpose and level of access.</li> <li>● Ensuring that non-escorted maintenance and cleaning personnel have completed the same training, screening and approval as authorized employees.</li> <li>● 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.</li> </ul>	
22	Facilities Maintenance Records	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
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: <ul style="list-style-type: none"> <li>● Located where they can safely and easily be accessed.</li> <li>● Protected from unauthorized or unintended activation.</li> </ul>	Low Moderate High
25	Emergency Power	Data centers must have: <ul style="list-style-type: none"> <li>● 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.</li> <li>● A long-term alternate power supply that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.</li> </ul>	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: <ul style="list-style-type: none"> <li>● All emergency exits and evacuation routes within the facility.</li> </ul>	Low Moderate High

		<ul style="list-style-type: none"> <li>All areas within the facility supporting essential missions and business functions.</li> </ul>	
27	Fire Protection	<p>Fire suppression and detection devices/systems must be in place that:</p> <ul style="list-style-type: none"> <li>Are supported by an independent energy source.</li> <li>Activate automatically.</li> <li>Notify facilities personnel and the local fire department in the event of a fire detection or suppression activation.</li> </ul>	<p>Low Moderate High</p>
28	Temperature and Humidity Controls	<p>Data centers must have controls in place to:</p> <ul style="list-style-type: none"> <li>Maintain temperature within the range from 64.4°F to 80.6°F.</li> <li>Maintain humidity within the range from 41.9°F Dew Point to 59°F Dew Point. Maintain Relative Humidity below 60%.</li> <li>Monitor temperature and humidity levels at least every 15 minutes.</li> </ul>	<p>Low Moderate High</p>
29	Water Damage Protection	<p>Data centers must have controls in place to prevent damage from water leakage by:</p> <ul style="list-style-type: none"> <li>Providing master shutoff or isolation valves that are accessible, working properly and known to data center facilities personnel.</li> <li>Using automated mechanisms to detect the presence of water in the data center and alert data center facilities personnel.</li> </ul>	<p>Low Moderate High</p>

### 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 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 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

Enterprise Physical and Environmental Security Policy

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

## History

Version	Description	Date
1.0	Initial Release	7/8/2015
1.1	Added Compliance Enforcement Date	12/29/2015

## Contact

**Information Security Risk Management Governance, Risk, and Compliance**

GRC@state.mn.us