

	Department of Administration Policy	Category	Physical and Environmental Protections, SITSD Security
		Effective Date	11/18/2009
		Last Revised	03/10/2015
Issuing Authority	State Information Technology Services Division		
POL-Physical and Environmental Protections Policy			

I. Purpose

The purpose of this Policy is to establish the requirement for the State Information Technology Services Division (SITSD) to implement Physical and Environmental Protection for information systems that SITSD manages or controls.

II. Scope

This Policy encompasses information systems that SITSD manages or controls, including systems that third-parties manage or host on SITSD's behalf.

III. Policy Statement

SITSD shall develop and implement Physical and Environmental Protection for the state's enterprise information systems maintained by SITSD based on the [National Institute of Standards and Technology \(NST\) SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#), and associated NIST guidelines and standards.

IV. Roles and Responsibilities

The following roles and responsibilities are required by this policy:

- A. Chief Information Officer:** Oversees the information technology resources that maintain information systems for SITSD.
- B. Chief Information Security Officer:** Ensures compliance with security policies and procedures within SITSD.

- C. Chief Technology Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- D. Chief Intergovernmental Relations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- E. Chief Operations Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- F. Chief Financial Officer:** Monitors organization compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.
- G. Division Personnel:** Responsible for implementation of requirements that are contained in policies and procedures.

V. Requirements

To support Physical and Environmental Protection, this Policy requires that SITSD shall:

1. Implement this Policy in compliance and integrated with guidance provided by the [National Institute of Standards and Technology Guidance](#).
Physical and environmental security controls are implemented to protect SITSD's facilities that house information systems, the information systems themselves, and the facilities to support the operation of SITSD information systems. Specific requirements for SITSD include:
 - a. Maintaining control of all physical access points to the facilities where information systems reside, also known as secured facilities, and completing a verification process for individual access authorizations before granting access to a facility.
 - b. Maintaining signage at the perimeter of secured facilities signifying an authorized access only location.
 - c. Restricting physical access to servers and network equipment to prevent tampering or accidental disruption of service.
 - d. Issuing credentials for access to secured facilities to personnel who need physical access to information systems on a day to day basis.

- e. Maintaining a list of personnel with authorized card key and biometric access to facilities where information systems reside.
- f. Maintaining control of physical access to information system distribution and transmission lines within secured facilities.
- g. Monitoring of physical access to the information systems to detect and respond to physical security incidents.
- h. Logging, escorting, and monitoring visitor access and activity.
- i. Protecting power equipment and power cabling for information systems from damage and destruction. The capability to shut off power to any information system component that may be malfunctioning or threatened must be provided by SITSD.
- j. Providing a short-term uninterruptible power supply to facilitate an orderly migration to an alternate power supply in the event of a primary power source loss.
- k. Maintaining automatic emergency lighting that activates in the event of a power disruption and that covers emergency exits and evacuation routes.
- l. Maintaining fire suppression and detection devices/systems that can be activated in the event of a fire.
- m. Monitoring of the temperature and humidity within the facility where the information systems reside, and being able to respond when either is not within established limits.
- n. Protecting information systems from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.
- o. Maintaining control of information system related items entering and exiting the facility and maintaining an appropriate record of these items.
- p. Positioning of information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
- q. Scheduling preventative maintenance on all environmental systems as required, to keep them in peak operating efficiency.
- r. Maintaining video surveillance of the State of Montana Data Centers and maintaining records as required.

2. Allocate adequate resources to maintain a physical and environmental protection program.
3. Review physical access configurations to SITSD facilities on an annual basis to ensure Policy and procedure compliance. Visitor access records will be included in this review.
4. Review the physical and environmental protection program, procedure(s), and associated documents on an annual basis. Necessary changes will be made as needed to support ongoing processes.

VI. Definitions

Refer to the [NIST Information Security Glossary of Key Information Security Terms](#) for a list of NIST definitions.

VII. Compliance

Compliance shall be evidenced by implementing the Physical and Environmental Protection Policy as described above.

VIII. Enforcement

Each bureau is responsible for the Policy's implementation and enforcement. The Chief Technology Officer, Chief Business Officer, and Chief Operations Officer shall monitor bureau compliance and may make enforcement recommendations to the appropriate level of management given the particular circumstances.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy can be found in the [MOM Policy System](#) (*search for: 261*). When considering formal disciplinary action, management will consult with their assigned Human Resource Specialist before taking action.

IX. References

A. Legislation

- [2-15-112 MCA](#) - Duties and Powers of Department Heads

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- SITSD Procedure: [PRO-IT Policies, Standards, Procedures and White Papers Procedure](#)

C. Standards, Guidelines

- [NIST SP800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations](#)