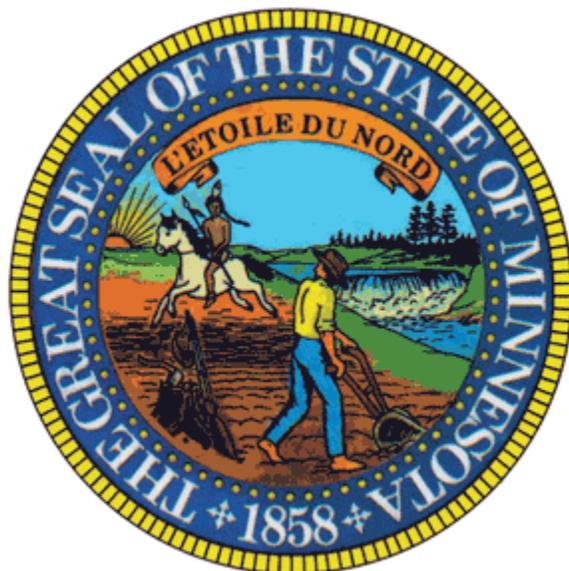


# State of Minnesota



## Enterprise Information Security Physical & Environmental Protection Standard

Office of Enterprise Technology

Enterprise Security Office Standard

Version 1.00

State CIO Standard Approval:

**Gopal Khanna**

<Signature on file with ESO>

03/24/2010

State Chief Information Officer

Signature

Approval Date



# Enterprise Security Office Standard

## Table of Contents

<b>1.0</b>	<b>STANDARD STATEMENT</b>	<b>3</b>
1.1	PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROL SELECTION	3
1.2	PHYSICAL AND ENVIRONMENTAL PROTECTION PROCEDURES	3
1.3	MINIMUM REQUIREMENTS FOR PHYSICAL PROTECTION	3
1.4	MINIMUM REQUIREMENTS FOR ENVIRONMENTAL PROTECTION	4
<b>2.0</b>	<b>ROLES &amp; RESPONSIBILITIES</b>	<b>4</b>
2.1	OFFICE OF ENTERPRISE TECHNOLOGY (OET)	4
2.2	GOVERNMENT ENTITY	4
<b>3.0</b>	<b>RELATED INFORMATION</b>	<b>5</b>
3.1	REASON FOR THE STANDARD	5
3.2	APPLICABILITY AND EXCLUSIONS	5
3.3	REGULATORY, POLICY, STANDARDS, & GUIDELINE REFERENCES	5
3.4	FORMS, TEMPLATES, AND PROCEDURES	5
3.5	COMPLIANCE	5
	<b>HISTORY &amp; OWNERSHIP</b>	<b>6</b>
	REVISION HISTORY – RECORD ADDITIONS AS MAJOR RELEASES, EDITS/CORRECTIONS AS MINOR	6
	REVIEW HISTORY – PERIODIC REVIEWS TO ENSURE COMPLIANCE WITH PROGRAM	6
	APPROVAL HISTORY – RECORD OF APPROVAL PHASES	6
	OWNERSHIP – CURRENT OWNERS OF THE DOCUMENT	6



## 1.0 Standard Statement

Government entities must implement the requirements in this standard to:

- limit physical access to information assets, information systems, and related equipment to authorized individuals;
- protect the facility and support infrastructure for information assets;
- protect information assets against natural disasters and environmental hazards; and
- provide the appropriate environmental controls and supporting utilities for information assets.

The following control requirements specify a minimum operating baseline common across all facilities containing state information assets.

### 1.1 Physical and Environmental Protection Control Selection

The selection of specific physical and environmental controls for a government entity's information assets must be based on a risk assessment process. This assessment must include, at a minimum, the criticality of the information assets, defined risks to those assets, and the strengths and constraints of the facility containing the assets.

When the criticality of individual information assets or the number of co-located assets (such as in a data center) increases, government entities must re-assess their physical security controls.

### 1.2 Physical and Environmental Protection Procedures

A government entity must have procedures to facilitate the implementation of the physical and environmental protection requirements in this standard.

At a minimum, procedures must be implemented at the entity level and at additional levels as necessary (e.g., facility, information asset, information system)

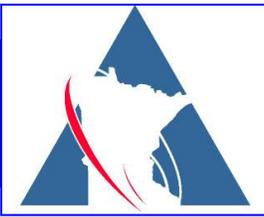
### 1.3 Minimum Requirements for Physical Protection

A government entity must implement<sup>1</sup> the following controls for facilities containing information assets, in accordance with the entity's assessment of risk:

1. Develop and keep current a list of personnel with authorized access to the facility (except for those areas officially designated as publically accessible), to include:
  - a. Issuing appropriate access rights and related physical security credentials (e.g. identification cards, badges, keys, combinations, codes);
  - b. Routinely review and approve the access list, rights, and credentials
  - c. Have procedures for timely termination of physical access rights and recovery of physical security credentials for voluntary termination of employment and job transfers; and
  - d. Promptly change physical access rights associated with an involuntary termination of employment and recover physical security credentials.
2. Restrict physical access to the facility to only authorized personnel by:
  - a. Verifying individual access authorizations before granting access to the facility;
  - b. Controlling entry to the facility using physical access devices (e.g. keys, locks, combinations, card readers) and/or guards;
  - c. Securing keys, combinations, and other physical access devices;
  - d. Routinely inventorying physical access devices; and

---

<sup>1</sup> Physical and/or environmental controls specified in this standard may be satisfied by similar requirements fulfilled by another organizational entity other than the information technology and/or security components.



## Enterprise Security Office Standard

- e. When physical access credentials are lost, stolen, or compromised physical security rights or corresponding devices must be promptly changed.
3. Control physical access to areas with critical or consolidated information assets (e.g. data centers, records storage areas):
  - a. Independently of the physical access controls for the facility; and
  - b. By limiting the number of personnel with physical access to the minimum necessary.
4. Control physical access to information system distribution and transmission lines.
5. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
6. Monitor physical access to the facility by:
  - a. Detecting and responding to physical security incidents;
  - b. Routinely reviewing physical access logs; and
  - c. Coordinating results of reviews and investigations with the entity's incident response capability.
7. Visitors must be authorized prior to accessing areas not publically accessible.

### 1.4 Minimum Requirements for Environmental Protection

A government entity must implement<sup>2</sup> the following controls for facilities containing information assets, in accordance with the entity's assessment of risk:

1. Protect power equipment and power cabling from damage and destruction.
2. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of critical information systems in the event of a primary power source loss.
3. Employ and maintain fire detection and suppression devices/systems within the facility where the information assets reside, supported by an independent energy source.
4. Monitor and maintain within acceptable levels the temperature and humidity within the facility where information assets reside.

## 2.0 Roles & Responsibilities

### 2.1 Office of Enterprise Technology (OET)

- Maintain this document and related standards, templates, and guideline documents.
- Fulfill the Government Entity roles and responsibilities for the Office of Enterprise Technology.

### 2.2 Government Entity

- Integrate the operational security requirements into established business processes.
- Maintain the necessary processes to address the security requirements of this standard.
- Report on operational security risks as necessary.
- Implement additional controls as necessary to address entity specific regulatory requirements.
- Periodically review physical and environmental controls for effectiveness.

---

<sup>2</sup> Physical and/or environmental controls specified in this standard may be satisfied by similar requirements fulfilled by another organizational entity other than the information technology and/or security components.



### 3.0 Related Information

#### 3.1 Reason for the Standard

In order to minimize disruption, damage, or loss of information and technology resources utilized by the Executive branch and to comply with the Enterprise Security Operational Control Policy, OP3 – Physical & Environmental Protection Policy, the minimum requirements for physical and environmental protection of information assets are identified in this standard.

Define the required standards for physical and environmental protection of facilities containing information assets or other technology resources to protect against threats that could cause a loss of confidentiality, integrity or availability of state information assets.

For the purposes of this standard, 'facilities' is defined to include all areas that contain information assets, including general workspace, but special focus should be placed on concentrations of assets, such as data centers, server rooms, network/data transmission hubs (i.e. telephone/data/wiring closets), concentrated cable runs, and technology or records staging/storage areas.

A guideline is available to provide additional recommendation for controls and other considerations for entities with more critical information assets or consolidated asset locations such as data centers.

#### 3.2 Applicability and Exclusions

This standard is applicable to the government entities in the Executive Branch identified in the [Enterprise Security Program Applicability Standard 2009-06](#). It is also offered as guidance to other government entities outside the Executive Branch.

Agency Heads, Responsible Authorities, Chief Information Officers, Chief Information Security Officers, Data Practices Compliance Officials, and their designees who are responsible for responding to, management of, and reporting on entity security controls must be aware of this standard.

The requirements of this standard must be incorporated into agreements with third parties to ensure proper physical and environmental controls are in place for protection of state information assets.

#### 3.3 Regulatory, Policy, Standards, & Guideline References

Minnesota Statutes 2007 Chapter 16E (Office of Enterprise Technology)  
Minnesota Statutes, Chapter 13 (Data Practices Act)

Enterprise Security Operational Control Policies  
Enterprise Physical and Environmental Protection Guideline

FIPS Publication 200  
NIST Special publication 800-14  
NIST Special Publication 800-53

#### 3.4 Forms, Templates, and Procedures

*Italicized* terms can be found in the Enterprise Security Glossary of Terms.

#### 3.5 Compliance

Compliance with this standard is required within 2 years of the approval date of the standard.



## Enterprise Security Office Standard

### History & Ownership

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
03/24/2010	Rick Ensenbach	Initial Release	1	00

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Aaron Molenaar Eric Breece Rick Ensenbach Clif Meier Enterprise Security Office Enterprise Security Office Enterprise Security Office Enterprise Security Office	09/01/2009
ISC	Information Security Council Approval	01/06/2010
CIO Council	CIO Council Approval	02/18/2010
State CIO	State Chief Information Officer, Gopal Khanna	03/24/2010

Ownership – current owners of the document

	Owner	Division	Department
Primary	Eric Breece	Enterprise Security Office (ESO)	Enterprise Security Governance
Secondary	Aaron Molenaar	Enterprise Security Office (ESO)	Enterprise Security Governance