



# State of Nevada

## Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.11	A	Physical Security and Environmental Controls	07/11/02	1 of 3

#### 1.0 PURPOSE

This standard establishes the minimum Information Technology (I/T) Physical Security and Environmental Controls standard for State information and information technology.

#### 2.0 SCOPE

This standard applies to all state agencies meeting the requirements identified in the State IT Security Policy, Section 2.0 Scope.

#### 3.0 EFFECTIVE DATES

The requirements of this standard are effective 90 days after sign-off by the Governor or his designee.

#### 4.0 RESPONSIBILITIES

The agency head or appointed Information Security Officer (ISO) has the responsibility to ensure the implementation of and compliance with this standard.

#### 5.0 RELATED DOCUMENTS

State IT Security Policy 4.02

State Information Security Officer (ISO) Roles and Responsibility, 4.03

National Institute of Standards and Technology (NIST), Special Publications:

800-12, An Introduction to Computer Security; the NIST Handbook, October 1995

800-14, generally Accepted Principles and Practices for Securing IT Systems, September 1996

#### 6.0 STANDARD

- A. Agencies are responsible for ensuring appropriate and cost effective physical security and environmental control standards and procedures are established and enforced.
- B. The agency Information Security Officer (ISO) shall in accordance with the I/T Security Policy, Section 5.0.2 G, review physical security and environmental control procedures annually or whenever facilities, environment, and/or security procedures are significantly modified and document review results.
- C. Agency management shall ensure that policies and procedures addressing emergency procedures relating to computer facilities, staff and all related equipment including computers, and environmental controls located throughout a building are in place.
- D. Agency management shall ensure that policies and procedures addressing physical security and environmental controls of all equipment used within the agency including responsibilities of all employees using such equipment is clearly identified.



# State of Nevada

## Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.11	A	Physical Security and Environmental Controls	07/11/02	2 of 3

- E. Agencies planning for new, remodeled or leased office construction shall ensure all appropriate physical security and related environmental controls and requirements are incorporated in the design.
- F. Physical security and environmental control factors to be considered for the location of computer facilities shall include, but not limited to the building location, source and grounding of electrical power, and the nature of the exteriors in regard to the safety of personnel.
- G. Mainframe computers, network servers, voice and network relays, telecommunications equipment, desktop computers and support peripheral devices shall be installed in physically secure and environmentally sound facilities or locations in accordance with industry and manufacturers standards.
- H. Physical access to controlled computer areas shall be restricted only to authorized personnel. Controlled computer areas shall be located in locked or secure rooms at all times. Authorized visitors shall be supervised and a record of their visits maintained.
- I. All computers, peripheral, media, data storage and network components outside the central computer room shall receive the level of security based on the criticality of the equipment and the data processed necessary to avoid damage, theft and/or unauthorized access and in accordance with industry and manufacturers standards.
- J. Electrical considerations in respect to the location of I/T equipment shall be considered, including but not limited to: avoidance of multiple systems on one electrical circuit, appropriate grounding, uninterruptible power supply units attached to critical systems and surge protectors on computer and peripheral equipment.
- K. Appropriate fire suppression devices shall be available and strategically located throughout the building and controlled computer areas.
- L. Water damage precautions shall be considered with respect to computer facilities and equipment.
- M. Management, staff and contracted employees are responsible for the proper usage, storage and disposal of hazardous materials and/or chemicals, including cleaning supplies used.
- N. Environmental controls shall be installed to ensure that the facility and equipment are maintained within optimum operating conditions including, but not limited to temperature, humidity and dust prevention.
- O. Environmental controls shall also provide for the safety of personnel.
- P. Controlled computer areas and related spaces, including but not limited to media and/or data storage and software libraries shall not be used as temporary storage rooms, lunch areas or warehouses. All equipment, floors and work surfaces shall be cleaned regularly.
- Q. Agency management or appointed ISO shall ensure backups of agency applications and data are stored, both on and off-site, in a secure manner.



# State of Nevada

## Information Technology Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.11	A	Physical Security and Environmental Controls	07/11/02	3 of 3

#### 7.0 DEFINITIONS

None

#### 8.0 EXCEPTIONS/OTHER ISSUES

Request for exception to the requirements of this IT Security Standard must be documented, provided to and approved by the State IT Security Committee and Chief Information Officer (CIO).

<i>Approved By</i>		
Title	Signature	Date
<b>State IT Security Committee Chair</b>	Signature on File	10/31/2001
<b>NV IT Operations Committee Chair</b>	Signature on File	07/11/2002
<b>Governor/Governor's Representative</b>	Signature on File	06/17/2003

<i>Document History</i>		
Revision	Date	Change
A	07/11/02	Initial release.