



# State of Nevada

## Information Security Committee

### Standard

---

Control No.	Rev.	Title	Effective Date	Page
4.11	B	Physical Security and Environmental Controls	3/14/12	1 of 3

---

#### 1.0 PURPOSE

This standard establishes the minimum physical and environmental controls standard for State information and information technology.

#### 2.0 SCOPE

This standard applies to all state entities, state employees, contractors and all other authorized users, including outsourced third parties, who have access to, use, store, transmit or manage state data or information within or for the Executive Branch of Nevada State Government.

#### 3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO) and the State IT Security Committee Chair/State CISO.

#### 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 Information Security Consolidated Policy 4.100000  
Information Security Officer (ISO) Roles and Responsibilities, 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 Security IT Systems, September 1996  
800-53, Recommended Security Controls for Federal Information Systems, August 2009

#### 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 Information Security Policy Section 4.01, 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.



# State of Nevada

## Information Security Committee

### Standard

---

Control No.	Rev.	Title	Effective Date	Page
4.11	B	Physical Security and Environmental Controls	3/14/12	1 of 3

---

- D. Agency management shall ensure that policies and procedures addressing physical security and environmental controls of all IT equipment used within the agency including responsibilities of all employees using such equipment are clearly identified.
- 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, mobile devices 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, and 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 and maintained in accordance with industry and manufacturers standards
- 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.



# State of Nevada

## Information Security Committee

### Standard

Control No.	Rev.	Title	Effective Date	Page
4.11	B	Physical Security and Environmental Controls	3/14/12	1 of 3

- 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 and maintained in accordance with industry and manufacturers standards.
- Q. Agency management or appointed ISO shall ensure backups of agency applications and data are stored, both on and off-site, and in a secure manner.
- R. All mobile devices must be secured and maintained in accordance with the level of sensitivity of the data that is processed and stored on the device and in accordance with the mobile device agreement that includes accordance with industry and manufacturers standards.

#### 7.0 EXCEPTIONS/OTHER ISSUES

Guidance for Exceptions is provided in State Information Security Policy, 4.100000, Appendix A

<i>Approved By</i>		
Title	Signature	Date
<b>State IT Security Committee</b>	Approved by Committee	1/26/12
<b>State IT Security Committee Chair/State CISO</b>	Signature on File	3/14/12
<b>State Chief Information Officer (CIO)</b>	Signature on File	3/14/12

<i>Document History</i>		
Revision	Date	Change
A	7/11/02	Initial release.
B	3/14/12	Renumbering and minor revisions.