State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.01.01	Enterprise Physical Security and Environmental Controls	F	12/31/2020	1 of 5

1.0 PURPOSE

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

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

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

5.0 RELATED DOCUMENTS

State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01

6.0 STANDARD

6.1 Physical Security Risk Management Plan

A. The following are the essential elements of physical security risk management:

1. List or definition of assets to be protected
2. List or definition of persons authorized for unescorted access
3. List of threats determined to pose a significant risk
4. Statement of an intended method for keeping the assets secured, allowing unescorted access only to authorized persons

B. All security decisions should be based on an assessment of risk. The benefits of any security measure should be balanced against the direct costs as well as the indirect costs (e.g. inconvenience and extra tasks) of security measures. ISOs are responsible for identifying and presenting risks and the value of mitigations and security enhancements to management. The business decision to accept or mitigate risk should be made at the highest level of the business when sensitive information or valuable assets are involved.

C. The minimum standard for any physical security method or implementation is that a breach of security will be immediately, easily, and directly observable. Preventing unauthorized access is the ideal, but detecting unauthorized access is paramount.

1. There are unusual methods and equipment that can breach many physical security implementations without leaving obvious traces. For the purposes of establishing a minimum-security standard, consider only the skills of an ordinary person, with a high degree of motivation, and the tools commonly and locally available.

2. Security measures chosen to protect assets should match the level of the threat to those assets. For instance, if a bad actor could be motivated to use lock pick skills and tools to obtain a high value asset, an agency should use RFID to secure the entrances, or use mitigating tools such as motion detectors and digital video recorders to ensure the agency is reasonably protected or at least aware of unauthorized access to secure sites.

6.2 Common Controls

A. Each agency site will have a written plan that addresses each of the essential elements of physical security listed in 6.1.A at a minimum. The plan will be reviewed at least annually, and the review will be documented.

B. The agency Information Security Officer (ISO) or their appointed representative shall perform an on-site review of physical security and environmental control procedures annually, or whenever facilities, environment, and/or security procedures are significantly modified, and document review results.

C. Agencies planning for new, remodeled, or leased office construction shall include the agency ISO during design phase requirements discussions and planning. Agencies will ensure all appropriate physical security controls and requirements are incorporated in the design.

D. The agency ISO or designee will verify the secure operation of controls at each entry point, for each site, annually. This includes all entry points, whether they are controlled by physical, electronic/technology, human, or other means. This review will be documented.

E. Visitors to secure areas will be escorted by an authorized person and a record of visits will be maintained for one year, at a minimum.

F. IT Infrastructure will not be directly accessible from public areas. This includes servers, communications equipment, plus low voltage and fiber optic data and voice cabling, and power and environmental infrastructure that serve the IT infrastructure. Infrastructure specifically built to interact with the public, such as a kiosk, is exempt from this requirement.

G. Computers, monitors, and other related equipment will not be placed so that active, usable data ports are within reach of members of the public. This includes USB, Ethernet, SCSI, serial, and any other ports capable of carrying data. The ports will be protected through physical placement of the device, measures that block port access such as port plugs or device cages, or software or other measures that prevent unauthorized use of the ports.

H. Monitors that are used to display controlled or confidential information will not be viewable from public areas. Covers that distort the screen image may be acceptable mitigations provided public spaces allow only angled views to the computer screen.

1. There is no distance limitation to this requirement since current technology can be used to successfully read a computer screen from hundreds of feet away.

2. Agency ISOs or designee will conduct annual audits of what can be viewed from public areas and through building windows.

6.3 IT Data Center Controls

A. 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.

B. Electrical considerations in respect to the location of IT 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.

C. 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

D. Water damage precautions shall be considered with respect to computer facilities and equipment including installation of leak detection devices (water).

E. 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.

F. Environmental controls shall also provide for the safety of personnel.

G. 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.

6.4 Communications Room Controls

A. 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.

B. Electrical considerations in respect to the location of IT equipment in the facility's designated communication room 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 when possible, and surge protectors on computer and peripheral equipment.

C. Appropriate fire suppression devices shall be available and strategically located in the communications room, and maintained in accordance with industry and manufacturers standards

D. Water damage precautions shall be considered with respect to the designated communications room and its associate equipment.

E. The building's environmental controls shall be monitored to ensure that the equipment in the communications room is maintained within acceptable operating conditions including, but not limited to, temperature, humidity and dust prevention.

F. A facility's designated communications rooms 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.

7.0 DEFINITIONS

Communications Room: A communications room is a small room that contains network and telecommunications systems and devices, and physical or virtual servers. It generally provides localized network and data services for the office or building in which it resides, as well as a connection into SilverNet or the agency's Wide Area Network. Communications Rooms are sometimes called Wiring Closets or Telecom Closets.

Data Center: A data center is the principal location that stores, processes and serves large amounts of mission-critical data. The location can include physical and virtual servers, storage subsystems, networking switches, routers and firewalls, as well as the cabling and physical racks used to organize and interconnect the IT equipment. The location must also contain an adequate infrastructure, such as power distribution and supplemental power subsystems, including electrical switching; uninterruptable power supplies; backup generators to include ventilation and cooling systems.

8.0 RESOURCES

NIST 800-53 Rev. 4, Security and Privacy Controls, April 2013 (Updated 1/22/2015)

9.0 EXCEPTIONS

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.01.01	Enterprise Physical Security and Environmental Controls	F	12/31/2020	5 of 5

Approved By

Title	Signature	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	11/24/2020
State Chief Information Officer (CIO)	Signature on File	11/30/2020

Document History

Revision	Effective Date	Change
A	7/11/2002	Initial release
B	3/14/2012	Renumbering and minor revisions
C	1/21/2015	Office of Information Security biennial review, replaces standard 4.11
D	2/22/2018	Updated Data Center controls, revisions of basic physical security
E	12/26/2018	Renumbering (106 to S.4.01.01) and compliance to ADA standards
F	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)