State of New Mexico Statewide Architectural Configuration Requirements Title: IT Physical Security Standard S-STD009.001 Effective Date: May 26, 2005

1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per Department of Information Technology Act, NMSA 9-27-1 et. seq. (1978).

2. Purpose

This standard defines requirements for protection of State IT assets and associated IT personnel from physical harm, theft, and/or destruction.

3. Scope

This applies to all agencies. Agency is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.

The Agency Chief Executive Officer (CEO), working in conjunction with the Agency Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each agency.

4. Standard

The following standards provide requirements that protect IT assets and associated IT personnel of the State of New Mexico from physical harm, theft, and/or destruction.

4.1. ACCESS TO PRIMARY FACILITIES HOUSING CRITICAL INFORMATION SYSTEMS: Information systems (mainframes, servers, etc.), media storage areas, and related communication wiring and network devices shall be located in secure locations (facility physical plant permitting) that are locked and restricted to access by authorized personnel only.

- Access to secured areas shall only be granted by the facility owner upon written request
- Facilities containing critical data or information shall be subject to access monitoring that establishes the identity of the person entering/exiting as well as the date and time of the access (e.g., recording badge information, videotaping) and provides data for auditing of physical access.

- Emergency exits to facilities housing critical information systems and related communication wiring and network devices shall be secured for re- entry of only authorized personnel.
- Where locking mechanisms with keypads are used to access secure areas, entry codes shall be changed periodically, according to a schedule defined by the agency.
- Where badge-reading systems are employed to log access into and out of a secure facility, "piggybacking" of badge holders shall be prohibited.
- Unused keys, entry devices, etc., shall be secured.
- At all times while inside secure facilities, unauthorized personnel shall be accompanied by authorized personnel. A paper access log shall be used to record the entrance and exit dates/times of all unauthorized personnel as well as the names of the authorized personnel accompanying them.
- Physical access to "critical" IT hardware, wiring, and network devices shall be in accordance with *Statewide Standard, Personnel Security S-STD-011*, and controlled by rules of least privilege necessary for the authorized employee or contractor to complete assigned tasks. Logical access to "critical" IT hardware and network devices shall be in accordance with *Statewide Standard, Account Management S-STD-001*.

4.2. ACCESS TO BACK-UP SYSTEMS: Physical access security measures employed for back-up systems/facilities shall be equivalent to those of the primary facilities.

4.3. ENVIRONMENTAL CONSIDERATIONS FOR PRIMARY FACILITIES HOUSING CRITICAL INFORMATION SYSTEMS: Information systems, media storage areas, and related communication wiring and network devices should be protected against loss or malfunction of environmental equipment or services necessary for the operation of the facility.

- Appropriate fire suppression and prevention devices should be installed and functioning according to manufacturer's specifications.
- Environmental (A/C) systems should be routinely maintained.
- Environmental facilities (A/C, heating, water, sewage, etc.) should be periodically inspected and reviewed for risk of failure.
- Locations of plumbing system lines should be known, and if possible, not in close proximity to "critical" IT devices, communication wiring, and network devices.
- Uninterruptible Power Systems (UPS) and backup generators shall provide a safeguard against loss of electrical power.

4.4. SAFEGUARDING IT EQUIPMENT AND REMOVABLE STORAGE MEDIA FROM THEFT/LOSS: Computing and telecommunications equipment shall be inventoried in accordance with *Statewide Standard, Configuration Management S-STD-002*, accounted for, and safeguarded from loss and resulting unauthorized use. Removable storage media (disk, tapes, CDs, etc.) should be consistently controlled and labeled to guard against misplacement and loss or unauthorized use of information.

- In accordance with stewardship requirements by Department of Finance and Administration, a fixed asset system including property identification numbers shall be used to provide physical control of State-owned IT assets and identify them if lost or stolen.
- Theft/loss of IT equipment may potentially result in the unintentional disclosure of confidential information. Agencies should communicate this secondary risk in additional to loss of the asset in their Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- Agencies should establish procedures to:
  - Consistently label removable storage media. Identifying labels should be free of descriptive information, which could disclose the contents.
  - Route the media with confirmation of receipt by the recipient.
  - Store media in compliance with manufacturer's storage requirements.

4.5 REVIEW OF PRIMARY FACILITY ACCESS AND ENVIRONMENTAL CONSIDERATIONS: Access and environmental considerations of primary facilities housing critical information systems should be reviewed and tested at least annually. Physical security requirements for access and environmental considerations should be evaluated each time there is a related security incident, significant alteration to the facility layout, or significant change to equipment/systems located at the facility.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

None

7. Attachments

None

8. Version Control

S-STD-009.001

9. Revision History

Original 5/26/05
Format Updated 09/18/13