

STATE of ARIZONA

Arizona Department Of Administration	Agency STANDARD A800-O2-S03 Rev 0	TITLE: <u>Physical Protection – Physical Access Control</u> Effective: February 15, 2008
---	--	---

1. AUTHORITY

- 1.1. The authority for this standard is based on the ADOA Policy A800 – IT Security.
- 1.2. Authority flows from the applicable Statewide Policies and Standards prepared by the Government Information Technology Agency (GITA).

2. PURPOSE

- 2.1. The purpose of this standard is to define the requirements for protection of State IT assets from physical harm, theft or destruction.
- 2.2. This standard recognizes ADOA Information Security’s (AIS) use of the Technology Infrastructure and Standards Assessment (TISA) as the instrument for determining compliance to ADOA and Statewide IT Policies and Standards.

3. SCOPE

- 3.1. This standard applies to all ADOA agency business units, including divisions, contractors or other entities using agency information technology resources and data.
- 3.2. The ADOA Director, in conjunction with the ADOA Chief Information Officer (CIO), is responsible for ensuring the effective implementation of ADOA Information Security Policy and Standards which reference the Statewide Information Technology Policies, Standards and Procedures (PSPs).

4. DEFINITIONS AND ABBREVIATIONS

- 4.1. None

5. STANDARD

- 5.1. Information systems, such as mainframes and servers, media storage areas, and communication wiring and network devices will be situated in secure locations that are locked and restricted to access by authorized personnel only.
 - 5.1.4. Access to secured areas will only be granted by the facility owner upon written request.
 - 5.1.5. Facilities containing critical data or information will 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.

- 5.1.6. Emergency exits to facilities housing critical information systems and related communication wiring and network devices will be secured for re-entry of only authorized personnel.
- 5.1.7. Where locking mechanisms with keypads are used to access secure areas, entry codes will be changed periodically, according to a schedule defined by the ADOA.
- 5.1.8. Where badge-reading systems are employed to log access into and out of a secure facility, “piggybacking” of badge holders is prohibited.
- 5.1.9. Unused keys and entry devices will be secured.
- 5.1.10. At all times while inside secure facilities, unauthorized personnel will be accompanied by authorized personnel. A paper access log will 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.
- 5.1.11. Physical access to critical IT hardware, wiring and network devices will be in accordance with ADOA Standard A800-O1-S01, Personnel Security, 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 will be in accordance with ADOA Standard A800-T2-S01, Access Control.

6. STANDARD NON-COMPLIANCE

- 6.1. All authorized users of ADOA Information Resources are responsible for understanding and adhering to this standard.
- 6.2. For non-compliance with this standard, all ADOA employees shall be subject to Human Resource progressive discipline, with the understood exception, that management may choose to take appropriate action commensurate with the seriousness of the offense.
- 6.3. Contractors and other authorized users will be held to contractual agreements

7. REFERENCES

- 7.1. ADOA Policy – A800, Information Security
- 7.2. ADOA Standard – A800-O1-S01, Personnel Security
- 7.3. ADOA Standard – A800-T2-S01, Access Control
- 7.4. Statewide Policy – P800, IT Security
- 7.5. Statewide Policy – P170, Privacy Policy

8. ATTACHMENTS

- 8.1. No attachments accompany this standard.