

Arizona Department Of Administration	Agency PROCEDURE A800-O2-S04-P2 Rev. 0	TITLE: <u>ADOA Disaster Recovery Data Center - Physical Access Control</u> Effective: January 19, 2010
---	---	---

1. AUTHORITY

- 1.1.** The authority for this Procedure is based on the ADOA Policy A800 – Information Security Policy and ADOA Standard A800-O2-S04, ADOA Data Center Physical Protection – Physical Access Control.

2. PURPOSE

- 2.1.** ADOA critical information resources such as mainframes, servers, media storage areas, communication wiring and network devices are situated in secure areas, restricted to badge access by authorized personnel only. The purpose of this procedure is to identify the steps for granting and removing access to the ADOA Disaster Recovery Data Center.

3. SCOPE

- 3.1.** This Procedure applies to all ADOA employees, contractors and other entities using ADOA Information Resources.

4. DEFINITIONS AND ABBREVIATIONS

- 4.1.** ADOA – Arizona Department of Administration
- 4.2.** AIS - ADOA Information Security
- 4.3.** AIS Manager – ADOA Information Security Manager
- 4.4.** ADOA Disaster Recovery Data Center – ADOA Data Center used for disaster recovery purposes, located at 400 W Congress in Tucson, AZ
- 4.5.** Restricted Access Door – Doors at entrances to rooms containing ADOA critical information resources and limit access to authorized personnel via electronic badge readers

5. PROCEDURE

5.1. Requesting Access for State Employees and Contractors

- 5.1.1.** The manager/supervisor (authorizing authority) and requesting person will complete and submit a written request for access utilizing ADOA’s Data Center Access Request Form. A copy can be found here:
<http://isd.azdoa.gov/sections/demand/security/forms.aspx> .
- 5.1.2.** Schedule the required security awareness training, i.e. Unauthorized Access (UNAX) and Health Insurance Portability

and Accountability Act (HIPAA) with AIS, by sending an email to Secadm@azdoa.gov.

- 5.1.3. AIS will review the access request for completeness, verify job requirements and determine and assign access accordingly.
- 5.1.4. Notification that access has been granted will be sent to the requestor and his/her manager or supervisor.
- 5.1.5. If additional access is required, a new request must be submitted to AIS for consideration.

5.2. Allowing Access for Vendors

- 5.2.1. Vendors requiring access will need to be escorted by an authorized employee/contractor.
- 5.2.2. Qwest employees will need to visit the Capital Police office (located in the same facility) to sign for the badge that allows Qwest personnel into the telephone closet.
- 5.2.3. Upon leaving the facility, the Qwest badge will be returned to the Capital Police Office and signed back in.

5.3. Removing Access for State Employees, Contractors and Vendors

- 5.3.1. Manager or supervisor (authorizing authority), will complete and submit a written request for removing access utilizing ADOA's Data Center Access Request Form. A copy can be found here: <http://isd.azdoa.gov/sections/demand/security/forms.aspx>.

5.4. Accessing restricted areas with your badge

- 5.4.1. Touch your badge to the badge reader at the door to the area you are attempting to access. Ensure the light on the reader turns green, allowing access.
- 5.4.2. Each employee/contractor with a badge will need to touch his or her badge to the reader – do not “piggy-back” by walking through the door behind a person who has just entered.
- 5.4.3. If you are escorting a person or persons without a badge, stay with them. **(Badges will not be shared).**
- 5.4.4. **Under no circumstances will Restricted Access Doors be propped open.**

5.5. Access Monitoring

- 5.5.1. Access activity within ADOA's Disaster Recovery Data Center is monitored via video cameras 24 hours a day, 7 days a week by Capital Police personnel manning the guard station at ADOA's Data Center in Phoenix.

5.5.2. Upon noting any access violations, the guard station at ADOA's Data Center in Phoenix will contact the Capital Police in Tucson and request they respond and secure the facility.

5.5.3. Violations will be investigated by AIS.

5.6. Access Log/Activity Review

5.6.1. Badge reader access logs are reviewed by AIS security personnel weekly to ensure terminated employees/contractors have been removed.

5.6.2. Badge reader activity logs are review by AIS security personnel weekly to verify each person that enters and exits the facility by date and time.

5.6.3. AIS Security personnel reviewing the log will notate their name, date and time of review.

5.7. Access Log/Activity Reporting

5.7.1. Managers will be provided Access Log/Activity Reports on a monthly basis.

5.7.2. The manager shall review the report and determine if the employee/contractor has the appropriate access to perform their duties.

5.7.3. If the employee's/contractor's level of access needs to be changed, the manager will submit a request by email to Secadm@azdoa.gov.

5.8. Access Log/Activity Report Retention

5.8.1. The Access Log/Activity Report that have been reviewed and notated will be retained for a period of three years.

6. REFERENCES

6.1. ADOA Policy A800 – Information Security

6.2. ADOA Standard A800-O2-S04, ADOA Data Center Physical Protection – Physical Access Control

7. ATTACHMENTS

7.1. None