ARIZONA DEPARTMENT OF ADMINISTRATION	**Agency** **POLICY**	**State of Arizona**

STATE DATA CENTER (SDC) PHYSICAL SECURITY

DOCUMENT NUMBER:	**ADOA– P6200**
EFFECTIVE DATE:	**OCTOBER 11, 2016**
REV:	**1.1**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 18-107.

2. PURPOSE

The purpose of this document is to promote access and physical security controls that safeguard equipment, personnel, and data in mission critical facilities and data centers managed and/or controlled by ADOA. [National Institute of Standards and Technology (NIST) 800-53 PE-1]

3. SCOPE

This policy applies to all Divisions of ADOA and IT integrations and/or data exchange with third parties that perform functions, activities or services for or on behalf of the Agency or its Divisions. Applicability of this policy to third parties is governed by contractual agreements entered into between ADOA and the third party/parties.

4. EXCEPTIONS

The Exception process allows Assistant Directors to make an informed decision on whether or not to request an exception to a particular SDC policy by understanding the risk and alternatives involved.

5. ROLES AND RESPONSIBILITIES

Note: The types of teams required are based on the definition of services available to the agencies.

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state BUs.

5.2 Chief Operating Officer (COO), Assistant Director, State Data Center Manager shall:

a. Shall oversee the management and operation of the State Data Center (SDC)

b. Shall make decisions, with respect to, the application of State policies and Arizona Revised Statutes to the SDC

c. Ultimate authority to ensure the delivery of contracted service delivery and support commitments, including but not limited to, making decisions regarding spending levels, acceptable risk, and interagency coordination of service events

d. Leads the SDC management team in its accomplishment of specific responsibilities critical to the delivery and support of SDC services

5.3 ADOA State Data Center Facility Operations Manager

a. Overall maintenance of all physical facilities

b. Managing planned maintenance for all physical facilities

c. Maintaining a resource budget for all environmental controls and electrical systems

d. Ensuring that all facilities comply with all applicable codes and laws (i.e., building and fire codes, ADA, etc.)

e. Forecasting additional resource requirements based on inputs from the data center manager, Operations Manager and other sources of information available from business units

5.4 ADOA State Data Center Operations Manager

a. Enforce security policies, procedures, and assisting the ADOA Security Manager in identifying exposures and risks with respect to data center operations.

b. Develop, implement and manage an asset control process that complies with State of Arizona General Systems Division (GSD) guidelines and provides for the identification and tracking of all physical assets under their area of cognizance.

c. Provide the facilities manager with physical operating characteristics for planned hardware platforms (weight, power, HVAC and special installation requirements).

d. Assist the Disaster Recovery/Business Continuity Manager with planning and systems tests and evaluation in support of disaster recovery and/or business continuity planning.

e. Ensure that physical operating characteristics are provided to the facilities manager in accordance with mutually agreed upon lead times.

f. Shall ensure users are appropriately trained and educated on SDC policies

g. Shall monitor employee activities to ensure compliance

5.5 ADOA Network and Infrastructure Managers

a. Provide the facilities manager with physical operating characteristics for planned communications hardware (weight, power, HVAC and special installation requirements) and cabling requirements.

b. Ensure that planned demarcations between ADOA Data Center networking and communications infrastructure and third part service providers comply with service provider interface specifications and that the interface specifications are consistent with technical standards and [any] applicable fire, safety and building codes.

5.6 ADOA Security Manager- Chief Information Security Officer CISO

a. Establish policies and procedures for physical security, Statewide P8260 Physical Security Controls Policy.

b. Provide the facilities manager with a list of physical security devices that need to be installed and implemented.

c. Provide the data center manager with requirements and procedures for maintaining physical security for the data center.

d. Coordinate security inspections and audits.

5.7 Individual ADOA SDC Users

a. Shall adhere to all state and ADOA policies, standards and procedures pertaining to the use of the State IT resources

5.8 State Data Center Security

a. Responsible for facilitating access to the State Data Center - 24/7/365
b. Validates authorization and ensures that only authorized individuals requesting entrance are allowed entrance
c. Distributes badges that identifies access authority for an individual
d. Provides key to lockers for all non-essential equipment that is not allowed on raised floor spaces
e. Ensures escort is available for all contractors and visitors.

6. POLICY

The principal objective of the SDC Physical Security Policy is to prescribe the industry best practices to SDC operations that will limit access to authorized personnel and minimize risk to SDC resources. [NIST 800-53]

6.1 **Physical Access Authorizations** - SDC shall: [NIST 800-53 PE-2] [Internal Revenue Service (IRS) Pub 1075] [Health Insurance Portability and Protection Act (HIPAA) 164.310 (a)(2)(iii)]

a. Develop and maintain a list of individuals with authorized access to controlled areas or facilities where the state information system resides;

b. Issue authorization credentials;

c. Review and approve the access list and authorization credentials quarterly;

d. Remove individuals from the access list when access is no longer required;

e. Require that managers are responsible for maintaining and updating their access list and updating the SDC with additions and deletions;

f. Conduct an onboarding personnel screening process;

g. Require that all staff and users having access to the SDC must attend annual security training (UNAX) [NIST 800-53 AT-3, 800-16, 800-50] [IRS Pub 1075];

h. Provide Basic Security Awareness Training to information system users with practical exercises that simulate cyber-attacks, and recognition and reporting of insider threats;

i. Provide Role Based Security Training to personnel with assigned security roles and responsibilities that includes practical exercises that reinforce training objectives in the following disciplines:

1) IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX)
2) Maintain a program that will record and track personnel security training compliance and require annual re-certification when required.

j. Restrict physical access to the facility containing any information system that processes classified information to authorized personnel with appropriate clearances and access authorizations. [NIST 800-53 PE-2, PE-3]

6.2 **Standard Physical Access Control** - SDC shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. Enforce physical access authorization at designated entry/exit points to the facility where the state information system resides [Payment Card Industry (PCI) 9.1];

b. Verify individual access authorizations before granting access to the facility [PCI 9.1, 9.3.1]; and

c. Control ingress/egress to the facility using keys, locks, combinations, card readers, and/or guards:

d. Require that all persons entering the Data Center must [NIST 800-53 PE-3]:

1) Possess a valid government issued photo ID;
2) Have authorization to access the facility;
3) Obtain authorization to bring computers, tools, tool bags, or diagnostic equipment prior to entry into the State Data Center facility.
4) Sign-in and out as required by the facility;
5) Display their SDC security badge at all times while in the facility;
6) Surrender their security badge, access cards, keys, SDC owned tools or phones prior to exiting the facility.

e. Employ cameras, monitoring by guards, or isolating selected state information system components to control access to areas within the facility.

6.3 **Protected Physical Access Control** - For all Protected state information systems and the server components of standard state information systems for which additional physical protections apply, SDC shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. Develop procedures to easily distinguish between onsite personnel and visitors. [PCI 9.2];

b. Give visitors a physical token that expires and that identifies the visitors as onsite personnel and ensure the visitor surrenders the physical token before leaving the facility or at the date of expiration; [PCI 9.3.2, 9.3.3.];

c. Escort visitors and monitor visitor activity within controlled areas;

d. Secure keys, combinations, and other physical access devices;

e. Inventory keys and other physical access devices every quarter; keys and other physical access devices assigned to visitors are inventoried every day; and

f. Change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

6.4 **Monitoring Physical Access** - SDC shall: [NIST 800-53 PE-6] [IRS Pub 1075]

a. Monitor physical access to the state data center to detect and respond to physical security incidents;

b. Review physical access logs periodically and upon occurrence of potential indications of events [PCI 9.1.1];

c. Coordinate results of reviews and investigations with the organizational incident response capability;

d. Employ security controls that include 24 x 7 security officer presence, sign-in procedures for all ingress and egress, managed key and access card plans, man trap, managed access permissions and access request methods [NIST 800-53 PE-6];

e. Maintain physical access logs for all individuals who enter the SDC with time/date stamps to provide traceability and correlation with any events requiring audits [NIST 800-53 PE-6] [PCI 9.4];

f. Store physical access monitoring data for at least three months [PCI 9.1.1];

g. Ensure that exterior Data Center doors shall be monitored and alarmed. [NIST 800-53 PE-6]; and

h. Employ Closed-circuit television (CCTV) cameras to monitor all areas of the facility including lobbies, common areas, customer lounge, data center floor space, admin areas, and engineering plant areas for your safety. All CCTV cameras shall be monitored and images retained. Violations noted by camera shall be addressed promptly. [NIST 800-53 PE-6] [PCI 9.1.1]

6.5 **Access Control** - SDC shall implement the following physical access controls:

6.5.1 Workstations - SDC shall implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users [HIPAA 164.310(b), 164.310(c)];

6.5.2 Tools, Diagnostic Equipment – SDC shall implement and provide secured locked cubicles for all bags, computers, phone, tools, or diagnostic equipment entering the facility that has not been preapproved to enter the facility;

6.5.3 Output Devices - SDC shall control physical access to state information system output devices to prevent unauthorized individuals from obtaining output [NIST 800-53 PE-5] [IRS Pub 1075].

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

8.1 ADOA Policy P100, Information Technology

8.2 ADOA Policy P8320, Access Control Policy

8.3 NIST Special Publication 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems

8.4 NIST Special Publication 800-53 Rev. 4. Security and Privacy Controls for Federal Information Systems

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
07/10/2014	Initial Release	1.0	Aaron Sandeen, State CIO and Deputy Director
10/11/2016	Updated all the Security Statutes	1.1	Morgan Reed, State CIO and Deputy Director