| | | |
|---|---|---|
| ARIZONA<br>DEPARTMENT<br>OF<br>ADMINISTRATION | **AGENCY**<br>**POLICY** | **State of Arizona** |

# P6200: STATE SHARED HOSTED DATA CENTER (SHDC) PHYSICAL SECURITY

| | |
|---|---|
| DOCUMENT NUMBER: | P6200 |
| EFFECTIVE DATE: | JULY 2, 2021 |
| REVISION: | 1.2 |

## 1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (the "Department"), the Department shall maintain a coordinated statewide plan for information technology (IT) implemented and maintained through policies, and adoption of statewide technical, coordination and security standards as authorized by Arizona Revised Statute (A.R.S.) § 18-104. The Department shall also formulate policies, plans and programs to effectuate the government information technology purposes of the department pursuant to A.R.S. § 18-104.

## 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. ROLES AND RESPONSIBILITIES

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

**4.1. State Chief Information Officer (CIO) shall:**

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

**4.2. Chief Operating Officer (COO), Cloud Ops Director, State Shared Hosted Data Center Manager shall:**

**4.2.1.** Oversee the management and operation of the State Shared Hosted Data Centers;

**4.2.2.** Make decisions, with respect to, the application of State policies and Arizona Revised Statutes to the SHDC;

**4.2.3.** Be the ultimate authority to ensure that contracted service delivery and support commitments are met, including but not limited to, making decisions regarding spending levels, acceptable risk, and interagency coordination of service events and decisions requiring their concurrence; and

**4.2.4.** Lead the SHDC management team in its accomplishment of specific responsibilities critical to the delivery and support of SHDC services.

**4.3. ADOA State Shared Hosted Data Center Manager**

**4.3.1.** Overall maintenance of all physical facilities

**4.3.2.** Managing planned maintenance for all physical facilities

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

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

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

**4.4. ADOA State Chief Security Officer**

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

**4.4.2.** Develop, implement and manage an asset control process that complies with Arizona Department of Administration General Services Division (ADOA-GSD) guidelines and provides for the identification and tracking of all physical assets under their area of cognizance.

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

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

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

**4.4.6.** Shall ensure users are appropriately trained and educated on SHDC policies.

**4.4.7.** Shall monitor employee activities to ensure compliance

### 4.5. ADOA Network and Infrastructure Managers

**4.5.1.** Provide the Shared Hosted Data Center facilities manager with physical operating characteristics for planned communications hardware (weight, power, HVAC and special installation requirements) and cabling requirements.

**4.5.2.** Ensure that planned demarcations between ADOA Data Center networking and communications infrastructure and third party 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.

### 4.6. ADOA State Chief Information Security Officer

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

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

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

**4.6.4.** Coordinate security inspections and audits.

### 4.7. Shared Hosted Data Center Tenants and Agency Users

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

### 4.8. State Shared Hosted Data Center Manager

**4.8.1.** Responsible for coordinating access to the Facility and the State Shared Hosted Data Center Space - 24/7/365

**4.8.2.** Facility owner validates authorization and ensures that only authorized individuals requesting entrance are allowed entrance into the Data Center facility

**4.8.3.** ADOA Shared Hosted Data Center Manager ensures that only authorized individuals requesting entrance are allowed into the facility

**4.8.4.** ADOA shall ensure escort is available for all contractors and visitors.

**4.8.5.** ADOA shall provide governance and audit oversight for all access to the Facility and State Shared Hosted Data Center

## 5. POLICY

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

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

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

**5.1.2.** Issue authorization credentials;

**5.1.3.** Review and approve the access list and authorization credentials quarterly;

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

**5.1.5.** Require that managers are responsible for maintaining and updating their access list and updating the SHDC with additions and deletions;

**5.1.6.** Conduct an onboarding personnel screening process;

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

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

**5.1.9.** 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:

**5.1.9.1.** IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX)

**5.1.9.2.** Maintain a program that will record and track personnel security training compliance and require annual re-certification when required.

**5.1.10.** 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, PE3]

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

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

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

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

**5.2.4.** Require that all persons entering the Data Center must [NIST 800-53 PE3]:

**5.2.4.1.** Possess a valid government issued photo ID;

**5.2.4.2.** Have authorization to access the facility;

**5.2.4.3.** Obtain authorization to bring computers, tools, tool bags, or diagnostic equipment prior to entry into the State Shared Hosted Data Center facility.

**5.2.4.4.** Sign-in and out as required by the facility;

**5.2.4.5.** Display their SHDC security badge at all times while in the facility;

**5.2.4.6.** Surrender their security badge, access cards, keys, SHDC owned tools or phones prior to exiting the facility.

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

**5.3.** **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, SHDC shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

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

**5.3.2.** 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.];

**5.3.3.** Escort visitors and monitor visitor activity within controlled areas;

**5.3.4.** Secure keys, combinations, and other physical access devices;

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

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

5.4. **Monitoring Physical Access** - SHDC shall: [NIST 800-53 PE-6] [IRS Pub 1075]Change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

**5.4.1.** Monitor physical access to the State Shared Hosted Data Center to detect and respond to physical security incidents;

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

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

**5.4.4.** 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];

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

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

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

**5.4.8.** 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]

**5.5.** **Access Control** - SHDC shall implement the following physical access controls:

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

**5.5.2.** Output Devices - SHDC 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].

## 6. DEFINITIONS AND ABBREVIATIONS

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

## 7. REFERENCES

**7.1.** ADOA Statewide Policy Framework P1050 - IT POLICIES, STANDARDS & PROCEDURES PROGRAM

**7.2.** ADOA Policy P8320, Access Control Policy

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

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

**7.5.** FBI Criminal Justice Information Services (CJIS) Security Policy Version 5.9 06/01/2020

**7.6.** IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information,2010.

## 8. ATTACHMENTS

None.

## 9. 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 | 1.0 | Morgan Reed, State CIO and Deputy Director |
| 06/21/2021 | Minor revisions to Iron Mtn and State Cage physical access procedures, added IRS Pub 1075 and FBI Criminal Justice Information Services (CJIS) references. | 1.2 | Randy Wheaton, ADOA ASET Director Cloud Ops & DC Infrastructure |
| 7/2/2021 | Approved | | J.R. Sloan, State CIO |