ARIZONA STATEWIDE INFORMATION SECURITY	**STATEWIDE POLICY**	**State of Arizona**

STATEWIDE POLICY (8260): PHYSICAL SECURITY PROTECTIONS

DOCUMENT NUMBER:	**(P8260)**
EFFECTIVE DATE:	**DRAFT SEPTEMBER 17, 2018**
REVISION:	**2.0**

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 as authorized by Arizona Revised Statutes (A.R.S.) § 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK P8260 PHYSICAL PROTECTIONS.

2. PURPOSE

The purpose of this policy is to protect agency information systems and assets through limiting and controlling physical access and implementing controls to protect the environment in which agency information systems and assets are housed.

3. SCOPE

3.1 Application to Budget Units (BUs) - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 Application to Systems - This policy shall apply to all agency information systems:

- **a. (P)** Policy statements preceded by "(P)" are required for agency information systems categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency information systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency information systems with protected healthcare information.
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency information systems with federal taxpayer information.

3.3 Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

1.1 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide Information Technology (IT) Policies, Standards and Procedures (PSPs) throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Technology PSPs within the (Agency) BU;

b. Ensure BU compliance with Physical Protections Policy; and

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.4 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of Agency Information Technology PSPs within the BU; and

b. Ensure Physical Security Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Agency Information Technology PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the Physical Protections Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the physical protection of agency information systems and assets.

5.6 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Physical Protections Policies; and

b. Monitor employee activities to ensure compliance.

5.7 Users of agency information systems shall:

a. Familiarize themselves with this policy and related PSPs; and

b. Adhere to PSPs regarding the physical protection of agency information systems and assets.

6. (AGENCY) POLICY

6.1 Physical Access Authorizations - The BU shall: [NIST 800-53 PE-2] [IRS Pub 1075] [HIPAA 164.310 (a)(2)(iii)] [PCI DSS 9.9, 9.3]

- **a.** Develop and maintain a list of individuals with authorized access to controlled areas or facilities where the agency information system resides;
- **b.** Issue authorization credentials based on job function; [PCI DSS 9.3]
- **c.** Review and approve the access list and authorization credentials quarterly; and
- **d.** Remove individuals access (including from the access list, keys, badges, and combination changes) when access is no longer required and immediately upon termination. [PCI DSS 9.3]

6.2 Standard Physical Access Control - The BU 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 agency information system resides; [PCI DSS 9.1]
- **b.** Verify individual access authorizations before granting access to the facility; [PCI DSS 9.1, 9.3.1]
- **c.** Control ingress/egress to the facility using keys, locks, combinations, card readers, and/or guards; and
- **d.** (P-PCI) Provide cameras, monitoring by guards, or isolating selected agency information system components (or any combination) to control access to areas within the facility officially designated as publically accessible. Review collected data and correlate with other entries. Store at least three (3) months unless otherwise directed by law. [PCI DSS 9.1.1]

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

- **a.** (P) Develop procedures to identify and authorize visitors [PCI DSS 9.4]
- **b.** (P) Develop procedures to easily distinguish between onsite personnel and visitors. [PCI DSS 9.2];
- **c.** (P) 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 DSS 9.4.2, 9.4.3.]

d. Escort visitors and monitors visitor activity within controlled areas; [PCI DSS 9.4.1]

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

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

g. Change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or separated.

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

a. Monitor physical access to the agency information system to detect and respond to physical security incidents;

b. (P) Use video cameras and/or access control mechanisms (or both) to monitor physical access to sensitive areas. [PCI DSS 9.1.1]

c. (P) Review physical access logs weekly and, upon occurrence of potential indications of events; [PCI 9.1.1]

d. (P) Coordinate results of reviews and investigations with the organizational incident response capability; and

e. (P) Store physical access monitoring data for at least three months. [PCI 9.1.1]

6.4.1 (P) **Intrusion Alarms/Surveillance Equipment** - The BU shall monitor real-time physical intrusion alarms and surveillance equipment. [NIST 800-53 PE-6(1)] [IRS Pub 1075]

6.4.2 (P-PCI) Inspect Payment Card Capture Devices - Periodically inspect device surfaces to detect tampering or substitution (for example, addition of card skimmers to devices, unexpected attachments or cables plugged into the device, missing, changed security labels, different colored casing, or changes to the serial number or other external markings). [PCI 9.9.2]

6.5 Visitor Control Records - The BU shall: [PCI DSS 9.4.4]

a. Maintain visitor access records to the controlled areas or facilities where the information system resides;

b. Review visitor access records monthly; [NIST 800-53 PE-8]

c. Maintain a visitor log that includes the visitor's name, the firm represented, and the onsite personnel authorizing physical access; and

d. The logs shall be retained for a minimum of three months. [PCI 9.1.1]

6.6 (P) **Access Control** - The BU shall implement the following physical access controls:

6.6.1 (P) **Transmission Medium** - The BU shall control physical access to agency information system distribution and transmission lines within BU facilities using locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays. [NIST 800-53 PE-4] [IRS Pub 1075]

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

6.6.3 (P) **Output Devices** - The BU shall control physical access to agency information system output devices to prevent unauthorized individuals from obtaining output. [NIST 800-53 PE-5] [IRS Pub 1075]

6.6.4 (P-PCI) **Network Jacks and Devices** - The BU shall restrict physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. [PCI 9.1.2, 9.1.3]

6.6.5 (P) **Power Equipment and Cabling** - The BU shall protect power equipment and power cabling for the agency information system from damage and destruction. [NIST 800-53 PE-9]

6.7 (P) **Power -** The BU shall implement the following physical controls for power:

6.7.1 (P) **Emergency Shutoff** - The BU shall: [NIST 800-53 PE-10]

- **a.** Provide the capability of shutting off power to the agency information system or individual system components in emergency situations;
- **b.** Place emergency shutoff switches or devices in data centers, server rooms, and computer rooms to facilitate safe and easy access for personnel; and
- **c.** Protect emergency power shut off capability from unauthorized activation.

6.7.2 (P) **Emergency Power** - The BU shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss. [NIST 800-53 PE-11]

6.8 **Emergency Lighting** - The BU shall employ and maintain automatic emergency lighting for the agency information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. [NIST 800-53 PE-12]

6.9 **Fire Protection** - The BU shall employ and maintain fire suppression and detection devices/systems for the agency information system that are supported by an independent energy source. [NIST 800-53 PE-13]

6.9.1 (P) **Detection Devices** - The BU shall employ fire detection devices/systems for the agency information system that activate automatically and notify the BU and emergency responders in the event of a fire. [NIST 800-53 PE-13(1)]

6.9.2 (P) **Suppression Devices** - The BU shall employ fire suppression devices/systems for the agency information system that provides automatic notification of any activation to the BU and emergency responders. [NIST 800-53 PE-13(2)]

6.9.3 (P) **Inspections** - The BU shall ensure the facility undergoes annual inspections by authorized and qualified inspectors and resolves identified deficiencies within 30 days. [NIST 800-53 PE-13(3)]

6.10 **Temperature and Humidity Controls** - The BU shall maintain defined temperature and humidity levels within the facility where the agency information system resides at data centers, server rooms and computer rooms; and monitors temperature and humidity levels daily. [NIST 800-53 PE-14]

6.11 **Water Damage Protection** - The BU shall protect agency information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. [NIST 800-53 PE-15]

6.12 **Delivery and Removal** - The BU shall authorize, monitor, and control agency information systems components entering and exiting the facility and maintains records of those items. [NIST 800-53 PE-16]

6.13 (P) **Alternate Work Site** - The BU shall: [NIST 800-53 PE-17]

- **a.** Define and employ minimum security controls at alternate work sites;
- **b.** Assess, as feasible, the effectiveness of security controls at alternate work sites; and
- **c.** Provide a means for employees to communicate with agency information security personnel in case of security incidents or problems.

6.14 (P) **Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for restricting physical access are documented, in use, and known to all affected parties [PCI DSS 9.10]

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK P8260 Physical Protections

8.2 Statewide Policy Exception Procedure

8.3 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

8.4 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.5 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.

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

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
9/01/2014	**Initial Release**	**Draft**	**Aaron Sandeen, State CIO and Deputy Director**
10/11/2016	**Updated all the Security Statutes**	**1.0**	**Morgan Reed, State CIO and Deputy Director**
9/17/2018	**Updated for PCI-DSS 3.2.1**	**2.0**	**Morgan Reed, State CIO and Deputy Director**