STATEWIDE POLICY (8320): ACCESS CONTROLS

DOCUMENT NUMBER:	**P8320**
EFFECTIVE DATE:	**January 30, 2025**
REVISION:	**5.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this policy is to define the correct use and management of logical access controls for the protection of agency systems and assets.

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 systems:

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

3.3 Federal Government Information - 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 - 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 - Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

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

Section Number	Exception	Rationale

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with statewide information security 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 Director the risk to state systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC) shall:

a. Advise the State CISO on matters related to Statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of agency information security PSPs within the BU;

b. Ensure BU compliance with Access Control Policy; and

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

5.5 BU Chief Information Officer (CIO) shall:

a. Work with the BU Director to ensure the correct and thorough completion of agency information security PSPs within the BU; and

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

5.6 BU ISO shall:

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

b. Ensure the development and implementation of adequate controls enforcing the Access Controls Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of agency systems and assets.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Access Control PSPs; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding correct use and management of logical access controls for the protection of agency systems and assets.

6. STATEWIDE POLICY

6.1 **Access Enforcement** - The BU shall ensure the agency system enforces approved authorizations for logical access to information and system resources in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST

800-53 AC-3] [HIPAA 164.308(a)(3)(ii)(A) - Addressable, 164.308 (a)(4)(ii)(B) & (C) - Addressable]

a. (P-PCI) BU shall conduct this review at least every six (6) months. [PCI DSS 7.2.4]

6.1.1 (P) **Assign Responsibility** - The BU shall assign to an individual or team the security management responsibility of monitoring and controlling all access to confidential data. [PCI DSS 12.5.5]

6.2 (P) **Develop Access Control Operational Procedures** - The BU shall develop daily operational security procedures for restricting access to sensitive data that are documented, in use, and known to all affected parties. [PCI DSS 7.3]

6.3 (P) **Information Flow Enforcement** - The BU shall ensure the agency system enforces approved authorizations for controlling the flow of information within the system and between connected systems based on BU-defined information flow control policies, including Statewide Policy Framework 8350: Systems and Communications Protections. These policies prohibit direct public access between the internet and any system component in the Protected agency system. [NIST 800-53 AC-4] [IRS Pub 1075] [PCI DSS 1.3]

6.3.1 (P) **Perimeter Firewalls for Wireless Networks** - The BU shall install perimeter firewalls between any wireless network and the protected agency system, and configures these firewalls to deny, or control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment into the protected agency system. [PCI DSS 1.2.3]

6.3.2 (P) **Personal Firewalls** - The BU shall require personal firewall software or equivalent functionality on any portable computing devices (including agency and/or employee-owned) that connect to the internet when outside the network (for example, laptops used by employees), and which are also used to access the agency network.. [PCI DSS 1.4]

6.4 (P) **Least Privilege** - The BU shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks. [NIST 800-53 AC-6] [IRS Pub 1075] [PCI DSS 7.1]

6.4.1 (P) **Organizational Isolation** - The BU shall implement policies and procedures that protect confidential information from unauthorized access by other (e.g., larger BU to which the BU is a part of) organizations. [HIPAA 164.308 (a)(4)(ii)(A)]

a. (P) **Shared Host Isolation** – For agencies that provide a shared hosting service to other agencies, the agency BU shall ensure that agency hosts are protected from other users and processes on the same host or environment. Specifically, that BU shall ensure that: [PCI DSS A.1]

b. each entity only runs processes that have access to that entity's own environment; [PCI DSS A.1.1] and

c. each entity's access and privileges shall be restricted to its own environment. [PCI DSS A.1.2]

6.4.2 (P) **Privileged Accounts** - The BU shall restrict access rights to privileged user accounts to least privileges necessary to perform job responsibilities. [PCI 7.1.1]

6.4.3 (P) **Job Classification** - The BU shall restrict access rights based on individual personnel's job classification and function. [PCI DSS 7.1.3]

6.5 (P) **Authorize Access to Security Functions** - The BU shall explicitly authorize access to the following security functions and security-relevant information: [NIST 800-53 AC-6(1)] [IRS Pub 1075]

a. Establishing system accounts;

b. Configuring access authorizations;

c. Setting events to be audited;

d. Setting intrusion detection parameters;

e. Filtering rules for routers and firewalls;

f. Cryptographic key management information; and

g. Configuration parameters for security services.

6.6 (P) **Non-Privileged Access for Non-Security Functions** - The BU shall require that users of agency system accounts, or roles, with access to security functions (e.g., privileged users), use non-privileged accounts or roles, when accessing non-security functions. [NIST 800-53 AC-6(2)] [IRS Pub 1075]

6.7 (P) **Log Use of Privileged Functions** - The BU shall include execution of privileged functions in the events to be logged by the agency system. [NIST 800-53 AC-6(9)]

6.8 (P) **Prohibit Non-Privileged Users From Executing Privileged Functions** - The BU shall ensure the agency system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. [NIST 800-53 AC-6(10)] [IRS Pub 1075]

6.9 **Unsuccessful Logon Attempts** - The BU shall ensure the agency system enforces a BU specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a BU specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with the Statewide Access Control Standard 8320. [NIST 800-53 AC-7] [PCI DSS 8.1.6]

6.10 System Use Notification - The BU shall ensure the agency system: [NIST 800-53 AC-8]

6.10.1 Displays to users a BU-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, executive orders, directives, policies, regulations, standards, and guidance and shall state the following: Users are accessing an agency system owned by the State of Arizona;

- **a.** Agency system usage may be monitored, recorded, and subject to audit;
- **b.** Unauthorized use of the agency system is prohibited and subject to criminal and civil penalties; and
- **c.** Use of the agency system indicates consents to monitoring and recording.
- **d.** Retains the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the agency system; and

6.10.2 For publicly accessible systems; the agency system shall also:

- **a.** Display to users the system use agency information before granting further access;
- **b.** Display to users references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- **c.** Include the notice given to public users of the agency system, a description of the authorized uses of the system.

6.11 (P) **Session Lock** - The BU shall ensure the agency system prevents further access to the system by initiating a BU specified limit of time inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures. If the user does not reestablish access within a BU specified limit of time the session is dropped. [NIST 800-53 AC-11] [IRS Pub 1075] [HIPAA 164.312 (a)(2)(iii)] [PCI DSS 8.1.7, 8.1.8]

6.11.1 (P) **Pattern-Hiding Display -** The BU shall ensure that the system conceals, via the device lock, information previously visible on the display with a publicly viewable image. [NIST 800-53 AC-11(1)]

6.11.2 (P) **Session Termination** - The BU shall ensure that the system automatically terminates a user session after BU-defined conditions or trigger events. [NIST 800-53 AC-12]

6.12 Permitted Actions Without Identification or Authentication - The BU shall identify user actions that can be performed on the agency system without identification or

authentication consistent with BU missions; and documents and provides support rationale in the security plan for the agency system, user actions not requiring identification or authentication. [NIST 800-53 AC-14]

6.13 **Remote Access** - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the agency system prior to allowing such connections. [NIST 800-53 AC-17]

6.14 (P) **Automated Monitoring / Control** - The BU shall ensure the agency system employs automated mechanisms to monitor and control remote access methods (e.g., detection of cyber-attacks such as false logins, denial of service-attacks, and compliance with remote access policies such as strength of encryption). [NIST 800-53 AC-17(1)] [IRS Pub 1075]

6.14.1 (P) **Security Using Encryption** - The BU shall ensure the agency system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-17(2)] [IRS Pub 1075] [PCI DSS 2.3, 4.1]

6.14.2 (P) **Managed Access Control Points** - The BU shall ensure the agency system routes all remote accesses through authorized and managed network access control points. [NIST 800-53 AC-17(3)] [IRS Pub 1075]

6.14.3 (P) **Privileged Access Commands** - The BU shall authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence, for BU-defined needs, and documents the rationale for such access in the security plan for the agency system. [NIST 800-53 AC-17(4)] [IRS Pub 1075]

- **a.** (P-PCI) Remote Access Technologies - BU shall implement technical controls to prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.

6.15 **Wireless Access** - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and authorizes wireless access to the agency system prior to allowing such connections that are consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-18]

6.15.1 (P) **Wireless Authentication and Encryption** - The BU shall ensure the agency system protects wireless access to the agency system using authentication of users and devices and encryption. [NIST 800-53 AC-18(1)] [IRS Pub 1075] [PCI DSS 4.1]

6.15.2 Wireless Encryption Strength – The BU shall ensure wireless networks transmitting confidential data use industry best practices to implement strong encryption for authentication and transmission. [PCI DSS 4.1.1]

6.15.3 (P) **Disable Wireless Networking** - The BU shall disable, when not in use, wireless networking capabilities embedded within system components prior to issuance and deployment. [NIST 800-53 AC-18(3)]

6.16 Access Control for Mobile Devices - The BU shall establish configuration guidance, connection requirements, and implementation guidance for BU controlled mobile devices to include when such devices are outside of controlled areas; and authorizes connection of mobile devices to agency systems. [NIST 800-53 AC-19]

6.16.1 (P) **Full Device Encryption** - The BU shall employ full-device or container-based encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to agency systems or to create, transmit or process confidential information. [NIST 800-53 AC-19(5)] [IRS Pub 1075] [HIPAA 164.308 (e)(2)(ii) - Addressable] [PCI DSS 4.1]

- **a.** (P-PCI) Primary Account Number Encryption - BU shall ensure a policy requiring if disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:
  1. On removable electronic media; or
  2. If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.
- **b.** (P-PCI) Primary Account Number Encryption - BU shall ensure a policy requiring if disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows:
  1. Logical access is managed separately and independently of native operating system authentication and access control mechanisms.
  2. Decryption keys are not associated with user accounts; and
  3. Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

6.16.2 (P) **Purge or Wipe Mobile Device** - The BU shall ensure that information on mobile devices are purged or wiped from mobile devices enabled for use with agency systems based on sanitization techniques using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250 after a BU-defined number of consecutive invalid logon attempts. [NIST 800-53 AC-7(2)]

6.17 Use of External Systems - The BU shall: [NIST 800-53 AC-20]

a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to access the system from external systems; and process, store, or transmit (agency) BU controlled information using external systems; or

b. Prohibit the use of BU-defined types of external systems.

6.17.1 (P) **Limits on Authorized Use** - The BU shall permit authorized individuals to use an external system to access the agency system to process, store, or transmit BU controlled information only after: [NIST 800-53 AC-20(1)] [IRS Pub 1075]

a. Verification of the implementation of controls on the external system as specified in the BU's information security and privacy policies and security and privacy plans; or

b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system in accordance with the Arizona State Library Records Retention Schedule, Management Records, Item 6: http://apps.azlibrary.gov/records/general_rs/Management.pdf.

6.17.2 (P) **Portable Storage Devices** - The BU shall restrict or prohibit the use of BU controlled portable storage devices by authorized individuals on external systems using BU defined restrictions. [NIST 800-53 AC-20(2)] [IRS Pub 1075]

6.17.3 (P) **Restricted Use of Non-BU Owned Systems** - The BU shall restrict the use of BU owned systems or system components to process, store, or transmit organizational information using BU-defined restrictions [NIST 800-53 AC-20(3)].

6.18 (P) **Information Sharing** - The BU shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access and use restrictions for BU-defined circumstances; and shall employ BU defined mechanisms or processes to assist users in making information sharing and collaboration decisions. [NIST 800-53 AC-21] [IRS Pub 1075] [PCI DSS 12.8]

6.18.1 (P) **Maintain List of Service Providers** - The BU shall maintain a list of service providers, including a description of the service provided, that have access to confidential data. [PCI DSS 12.8.1]

6.18.2 (P) **Written Agreements** - The BU shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of confidential data the service providers possess. [PCI DSS 12.8.2]

6.18.3 (P) **Due Diligence** - The BU shall ensure there is an established process for engaging service providers including proper due diligence prior to engagement. [PCI DSS 12.8.3]

6.18.4 (P) **Service Provider Monitoring Program** - The BU shall maintain a program to monitor service provider's compliance with requirements for the protection of confidential data. [PCI DSS 12.8.4]

6.18.5 **(P) Service Provider Information** - The BU shall maintain information about which information security requirements are managed by each service provider, and which are managed by the BU. [PCI DSS 12.8.5]

6.19 **Publicly Accessible Content** - The BU shall: [NIST 800-53 AC-22]

- **a.** Designate individuals authorized to make information publicly accessible system;
- **b.** Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- **c.** Review the proposed content of information prior to posting onto the publicly accessible agency system to ensure that nonpublic information is not included; and
- **d.** Review the content on the publicly accessible agency system for nonpublic information annually and remove such information, if discovered.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8320 Access Controls

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections

8.4 Statewide Standard 8320, Access Control

8.5 Statewide Standard 8350, System Communication and Protection

8.6 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

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

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

8.9 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

8.10 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number GS 1005, Arizona State Library, Archives and Public Records, Item Number 6

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 of Arizona CIO and Deputy Director**
5/26/2021	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer**
1/16/2024	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**
1/30/2025 **2/11/2025**	**Annual Updates**	**5.0**	**Errika Celsy, Chief Privacy and Compliance Officer;** **Deputy Director Department of Homeland Security & State Chief Information Security Officer**