	STATEWIDE **POLICY**	**State of Arizona**

STATEWIDE POLICY (8310): ACCOUNT MANAGEMENT

DOCUMENT NUMBER:	**P8310**
EFFECTIVE DATE:	**January 16, 2024**
REVISION:	**4.0**

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.)§ 18-104 and § 18-105.

2 PURPOSE

The purpose of this policy is to establish the baseline controls for the administration of agency system accounts.

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 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 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	Explanation / Basis

5 ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of statewide 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 all state BU activities and documentation provided to ensure compliance with Statewide Information Security PSPs throughout all state BUs;

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing 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)

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 BU PSPs;

b. Ensure compliance with BU PSPs; and

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

5.5 BU CIO shall:

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

b. Ensure BU PSPs are 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 BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to secure account management.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU 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 account management and acceptable use of agency systems.

STATEWIDE POLICY

6. The BU shall implement account management through the following activities:

6.1. (P) **Automated Account Management** - The BU shall support the management of system accounts using automated mechanisms. [NIST 800-53 AC-2(1)] [IRS Pub 1075]

6.2. (P) **Develop Account Management Operational Procedures** - The BU shall ensure that security policies and operational procedures for restricting access to Confidential data are documented, in use, and known to all affected parties and cover all system components. [PCI DSS 7.2.1, 7.3]

6.3. **Identify Account Types** - The BU shall define and document the types of agency system accounts (e.g., individual, guest, emergency access, developer, maintenance, administration) allowed and specifically prohibited for use within the system. . [NIST 800-53 AC-2a] [HIPAA 164.312 (a)(2)(iii) – Addressable] [PCI DSS 7.2.2]

6.3.1. **Establish Group and Role-based Accounts** - The BU shall require BU-defined prerequisites and criteria for group and role membership. [NIST 800-53 AC-2c] [PCI DSS 7.1.1] [PCI DSS 7.2.2]

6.3.2. **Account Specification** -The BU shall specify authorized users of the agency system, group and role membership, and access authorizations (i.e., privileges) and other BU-defined attributes for each account. [NIST 800-53 AC-2d] [PCI DSS 7.1.3]

6.3.3. (P) **Privileged Accounts** - The BU shall restrict privileged accounts (e.g., super user accounts) on the agency system to administrative roles. [NIST 800-53 AC-6(5)] [IRS Pub 1075] [PCI DSS 7.1.2]

6.3.4. (P) **Separation of Duties** - The BU shall identity and document (Agency) BU -defined duties of individuals requiring separation and and define agency system access authorizations to support separation of duties. [NIST 800-53 AC-5] [IRS Pub 1075] [PCI DSS 6.4.2]

6.4. **Assign Account Managers** - The BU shall assign account managers for agency systems. [NIST 800-53 AC-2b]

6.5. Account Approval - The BU shall require documented approvals by authorized BU staff for requests to create, modify, and enable agency system accounts. [NIST 800-53 AC-2e-f] [PCI DSS 7.1.4]

6.5.1. (P) **Automated Audit Actions** - The BU shall ensure the agency system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required, BU-defined personnel or roles. [NIST 800-53 AC-2(4)] [IRS Pub 1075]

6.6. Account Monitoring - The BU shall authorize, and monitor the use of agency system accounts. [NIST 800-53 AC-2g]

6.6.1. (P) **Vendor Account Monitoring** - The BU shall enable accounts used by vendors for remote access only during the time period needed and monitors the vendor remote access accounts when in use. [PCI DSS 8.1.5]

6.7. Account Creation, Deletion, and Removal – The BU shall control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. {PCI DSS 8.1.2]

6.7.1. Account Removal - The BU shall notify account managers within 24 hours when accounts are no longer required; users are separated or transferred; and individual system usage or need-to-know changes. [NIST 800-53 AC-2h] [PCI DSS 8.1.3]

6.7.2. (P) **Immediate Removal of Separated Users** - The BU shall immediately revoke access for any separated users. [PCI DSS 8.1.3]

6.7.3. (P) **Automatic Removal of Temporary Accounts** - The agency system automatically removes or disables temporary and emergency accounts when the accounts have expired, are no longer associated with a user or individual. are in violation of organizational policy, or have been inactive for a BU-defined time. [NIST 800-53 AC-2(2)] [IRS Pub 1075]

6.7.4. (P) **Disable Accounts** - The BU shall ensure the agency system:

a. Automatically disable inactive accounts after BU -defined time period. [NIST 800-53 AC-2(3)] [IRS Pub 1075]

b. (P-PCI) For agency systems containing cardholder data (CHD) the time period must be no more than 90 days. [PCI DSS 8.1.4]

c. Disables accounts of individuals within 24 hours of discovery of BU-defined significant risks (e.g., intention to use authorized access to systems to cause harm). [NIST 800-53 AC-2(13)]

6.7.5. (P) **Inactivity Logout** - The BU shall ensure that users log out when a BU-defined time-period of expected inactivity is exceeded. [NIST 800-53 AC-2(5)]

6.8. **Access Authorization** - The BU shall authorize access to the agency system based on a valid access authorization; intended system usage; and other attributes as required by the organization or associated mission functions. [NIST 800-53 AC-2i] [HIPAA 164.308 (4)(ii)(B) – Addressable] [PCI DSS 7.1, 7.2]

6.8.1. (P) **Default "Deny-All" Setting** - The BU shall ensure the agency system access control system is set to "Deny all" unless specifically allowed. [PCI DSS 7.2.3]

6.8.2. (P) **Restrict Direct Database Access** - The BU shall ensure the agency system authenticates all access to any database containing Confidential information and restricts direct access or queries to databases to database administrators. [PCI DSS 8.7]

6.9. **Accounts Rights Review** - The BU shall review the privileges assigned to accounts to validate the need for such privileges and for compliance with account management requirements annually. The BU shall reassign or remove privileges, if necessary, to correctly reflect BU mission and business needs. [NIST 800-53 AC-6(7)] [HIPAA 164.308 (4)(ii)(C) – Addressable]

6.10. **Reissues Account Credentials** - The BU shall establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group. [NIST 800-53 AC-2k]

6.11. **Align with Termination Process** - The BU shall align the account management processes with personnel termination and transfer processes. [NIST 800-53 AC-2i]

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 8310 Account Management

8.2. Statewide Policy Exception Procedure

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

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

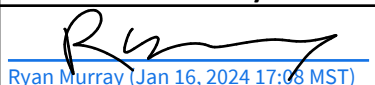
8.5. Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.

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

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 (Jan 16, 2024 17:08 MST) **Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

P8310_Account_Management (1)

Final Audit Report 2024-01-17

Created:	2024-01-16
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIrezD985y2Fipx-ja6p3GtZhmI0SQkO-

"P8310_Account_Management (1)" History

Document created by Ed Yeargain (eyeargain@azdohs.gov)
2024-01-16 - 11:38:55 PM GMT

Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature
2024-01-16 - 11:39:41 PM GMT

Document e-signed by Ryan Murray (rmurray@azdohs.gov)
Signature Date: 2024-01-17 - 0:08:45 AM GMT - Time Source: server

Agreement completed.
2024-01-17 - 0:08:45 AM GMT