



STATEWIDE POLICY



State of Arizona

STATEWIDE POLICY (8340): IDENTIFICATION AND AUTHENTICATION

DOCUMENT NUMBER:	P8340
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.)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this policy is to define the security requirements for establishing and maintaining user accounts for agency systems.

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 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)

- 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 Identification and Authentication 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 Identification and Authentication 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 Identification and Authentication Policy for the BU; and
- c. Ensure all personnel understand their responsibilities with respect to establishing and maintaining user accounts for agency systems.

5.7 Supervisors of agency employees and contractors shall:

- a. Ensure users are appropriately trained and educated on Identification and Authentication Policies; 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 the establishment and maintenance of user accounts for agency systems.

6. STATEWIDE POLICY

- 6.1.1 Identification and Authentication of Organizational Users** - The BU shall ensure the agency system **uniquely** identifies and authenticates organizational users and associate that unique identification with processes acting on behalf of those users. [NIST 800 53 IA-2] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]
- 6.1.2 Access to Privileged Accounts** - The BU shall ensure the agency system implements multifactor authentication for access to privileged accounts. [NIST 800 53 IA-2(1)] [IRS Pub 1075]
- 6.1.3 Access to Non-Privileged Accounts** - The BU shall ensure the agency system implements multifactor authentication for access to non-privileged accounts. [NIST 800 53 IA-2(2)] [IRS Pub 1075]
- 6.1.4 (P) Network Access to Privileged Accounts – Replay Resistant** - The BU shall ensure the agency system implements replay-resistant authentication mechanisms for access to privileged accounts. [NIST 800 53 IA-2(8)]
- 6.1.5 Access to Accounts (Privileged and Non-Privileged) – Separate Device** - The BU shall ensure the agency system implements multifactor authentication for remote access to organizational accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets statewide cryptographic standards for strength of mechanism. [NIST 800 53 IA-2(6)] [PCI DSS 8.3, 8.3.1] [IRS Pub 1075]
- 6.2 (P) Device Identification and Authentication** - The BU shall ensure the agency system uniquely identifies and authenticates before establishing a local, remote, or network connection. [NIST 800 53 IA-3] [IRS Pub 1075] [HIPAA 164.312 (d)]
- 6.3 Identifier Management** - The BU shall manage the agency system identifiers by: [NIST 800 53 IA-4] [PCI DSS 8.5]
 - a. (P) Ensuring that group, shared, or generic account identifiers and authentication methods are not used; [PCI DSS 8.5, 8.6]
 - b. Receiving authorization from BU-defined personnel or roles to assign individual, role, service, or device identifier;
 - c. Selecting an identifier that identifies an individual, role, service, or device;
 - d. Assigning the identifier to the intended individual, role, service, or device;
 - e. Preventing reuse of identifiers for one year; and
 - f. Disabling the identifier after 90 days of inactivity. [PCI DSS 8.1.4]

6.3.1 Identify User Status - The BU shall manage individual identifiers by uniquely identifying each individual with a BU-defined dynamic identifier policy. [NIST 800 53 IA-4(4)]

6.4 Authenticator Management - The BU shall manage the agency system authenticators (e.g., passwords, tokens, certificate, and key cards) by: [NIST 800 53 IA-5] [HIPAA 164.308(a)(5)ii(D)] [HIPAA 164.308 (d)]

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; [PCI DSS 8.2.2]
- b. Establishing initial authenticator content for authenticators issued by the BU;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators prior to first use;
- f. Changing or refreshing authenticators BU-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI certificates, and key cards) or when a suspected compromise occurs;
- g. Protecting authenticator content from unauthorized disclosure and modification;
- h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; [PCI DSS 8.6]
- i. Changing authenticators for group or role accounts when membership to those accounts changes; and
- j. Employing at least one of the following methods to authenticate all users: [PCI DSS 8.2]
 1. Password-Based Authentication
 2. PKI-based Authentication
 3. In Person or Trusted Third Party Registration
 4. Hardware Token-based Authentication

6.4.1 Password-Based Authentication - The BU shall ensure the agency system, for password-based authentication enforces password controls consistent with the

Statewide Standard 8340, Identification and Authentication. [NIST 800 53 IA-5(1)] [PCI DSS 8.2.3, 8.2.4, 8.2.5, 8.2.6]

- a. **Password Encryption** - The BU shall ensure the use of strong cryptography and render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. [PCI DSS 8.2.1]

6.4.2 (P) Public Key-based Authentication - The BU shall ensure the agency system, for Public Key-based authentication: [NIST 800 53 IA-5(2)] [IRS Pub 1075]

- a. For public key-based authentication:
 - 1. Enforces authorized access to the corresponding private key;
 - 2. Maps the authenticated identity to the account of the individual or group; and
- b. When public key infrastructure (PKI) is used:
 - 1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
 - 2. Implements a local cache of revocation data to support path discovery and validation.

6.4.3 Protection of Authenticators - The BU shall protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. [NIST 800 53 IA-5(6)]

6.5 Authenticator Feedback - The BU shall ensure the agency system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. [NIST 800 53 IA-6]

6.6 Cryptographic Module Authentication - The BU shall ensure the agency system implements mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. [NIST 800 53 IA-7]

6.7 Identification and Authentication (Non-Organizational Users) - The BU shall ensure the agency system uniquely identifies and authenticates non-organizational users or processes acting on behalf of non-organizational users. [NIST 800 53 IA-8] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]

6.7.1 Acceptance of External Authenticators - The BU shall ensure the agency system accepts only external authenticators that are NIST-compliant; and

document and maintain a list of accepted external authenticators. [NIST 800 53 IA-8(2)]

6.7.2 Use of Defined Profiles - The BU shall ensure the agency system information system conforms to the BU-defined identity management profiles. [NIST 800 53 IA-8(4)]

6.8 Re-Authentication - The BU shall ensure the agency system requires users to re-authenticate when the following circumstances or situations requiring re-authentication occur: [NIST 800 53 IA-11]

- a. change in role, authenticators, or credentials;
- b. execution of BU-defined privileged functions; or
- c. after a BU-defined period of time.

6.9 (P) Identity Proofing - The BU shall identity proof (the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system) users that require accounts for logical access to agency systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; resolve user identities to a unique individual; and collect, validate, and verify identity evidence. [NIST 800 53 IA-12]

6.9.1 (P) Identity Evidence - The BU shall require evidence of individual identification be presented to the registration authority. [NIST 800 53 IA-12(2)]

6.9.2 (P) Identity Evidence Validation and Verification - The BU shall require that the presented identity evidence be validated and verified through BU-defined methods of validation and verification. [NIST 800 53 IA-12(3)]

6.9.3 (P) Address Confirmation - The BU shall require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record. [NIST 800 53 IA-12(5)]

6.10 (P) Develop Operational Procedures - The BU shall ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 8.4, 8.8]

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

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 8340 IDENTIFICATION AND AUTHENTICATION
- 8.2 Statewide Policy Exception Procedure
- 8.3 Statewide Standard 8340, Identification and Authentication
- 8.4 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020..
- 8.5 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006
- 8.6 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.
- 8.7 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 17:43 MST)

			Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer
--	--	--	--------------------------------------------------------------------------------------------------------------------





P8340_Identification_Authentication (1) (1)

Final Audit Report

2024-01-17

Created:	2024-01-17
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAfV2qlerYDoHoulqtFnewHhGMvLSMMUjL

"P8340_Identification_Authentication (1) (1)" History

-  Document created by Ed Yeargain (eyeargain@azdohs.gov)
2024-01-17 - 0:41:12 AM GMT
-  Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature
2024-01-17 - 0:42:03 AM GMT
-  Document e-signed by Ryan Murray (rmurray@azdohs.gov)
Signature Date: 2024-01-17 - 0:43:18 AM GMT - Time Source: server
-  Agreement completed.
2024-01-17 - 0:43:18 AM GMT