	STATEWIDE # STANDARD	**State of Arizona**

STATEWIDE STANDARD (8340): IDENTIFICATION AND AUTHENTICATION

DOCUMENT NUMBER:	**S8340**
EFFECTIVE DATE:	**April 5, 2024**
REV:	**1.1**

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 standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

3.1 Application to Budget Units - This standard applies to all Budget Units (BUs). A BU is defined as a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 18-101(1).

3.2 Application to Systems - This standard shall apply to all state information 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.

a. 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.

b. 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	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 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 STANDARD

6.1 Identifier Management – The BU shall manage the state information system identifiers* by: [NIST 800 53 IA-4] [PCI DSS 8.5, 8.5.1]

- **a.** **(P)** Ensuring that group, shared, or generic account identifiers and authentication methods are not used; [PCI DSS 8.5.8]
- **b.** Receiving authorization from BU defined personnel or roles to assign individual, role, or device identifier;
- **c.** Selecting an identifier that identifies an individual, role, or device;
- **d.** Assigning the identifier to the intended individual, role, or device;
- **e.** Preventing reuse of identifiers for three years; and
- **f.** Disabling the identifier after 90 days of inactivity. [PCI DSS 8.5.5]

a. The enterprise identifier, Employee Identification Number (EIN), is created as a non-protected identifier for a specific employee, contractor, or volunteer as opposed to using the SSN or DOB. The non-protected EIN must not be used for any purpose to change or alter the status of a public classification.

6.2 Password-Based Authentication – The state information system, for password-based authentication shall: [NIST 800 53 IA-5(1)]

- **a.** Store and transmit only encrypted representation of passwords;
- **b.** Allow the use of a temporary password, unique to each user, for system logons with an immediate change after first use to a permanent password; [PCI DSS 8.5.3]
  - The content of these temporary passwords shall not be reused. [NIST 800-63B]
- **c.** Store passwords (and other memorized secrets) in a form that is resistant to offline attacks. These stored secrets shall be salted (at least 32 bits) and hashed using a suitable key derivation functions (e.g., HMAC, SHA-3, CMAC, KMAC, cSHAKE, of ParallelHash); [NIST 800-63B] and
- **d.** Utilize the following password authentication parameter settings:

Password Authentication Parameter	Setting Requirement
Enforce Minimum Password Complexity	• Twelve (12) characters, • Mix of upper-case letters, lower-case letters, numbers, and a special character. [IRS Pub 1075]
Enforce Password Maximum Lifetime Restrictions	• 90 days maximum [PCI DSS 8.2.4] • 60 days maximum for Administrator and Privilege Accounts [IRS Pub 1075]

Enforce Password Minimum Lifetime Restrictions	• 1 day minimum [IRS Pub 1075] • (P-FTI) -15 day minimum
Prohibit Password Reuse	• Twenty Four (24) generations [IRS Pub 1075]

e. Alternative Password Authentication Parameter Settings: Optionally, the BU may adopt the following alternative password authentication parameters: [NIST 800-63B]

Password Authentication Parameter	Setting Requirement
Hints and Security Questions	• Hints or stored information intended to remind the user of the password shall not be permitted. • The system shall not prompt the user to use specific information when establishing passwords (e.g., security questions).
Password Strength Meter	• The system shall offer the user guidance (e.g., strength meter) as to the strength of the selected password.

Rate Limiting	• The system shall limit password guessing by:
	  • Limiting consecutive attempts on a single account to 10
	  • (Optional) Require completion of a CAPTCHA prior to attempting authentication
	  • (Optional) Require an increasing wait time after each successive failed attempt, starting with 30 seconds and up to 1 hour.

Password Change	• The system shall not require the periodic changing of passwords. • The system shall allow the user to change their password when the user suspects a compromise. • The BU shall force a change of password when there is evidence of a compromise.
Password System Functions	• (Optional) The system shall allow the user to use the paste function when entering the password.
	• (Optional) The system shall provide the user an option to display the password until it is entered. • (Optional) The system shall allow the user's device to display individual characters for a short time after each character is typed to verify correct entry.

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 NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management, National Institute of Standards and Technology, U.S. Department of Commerce, March 2020.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
05/26/2021	**Annual Updates**	**1.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer** *Tim Roemer* Tim Roemer (May 25, 2021 22:08 PDT)
04/05/2024	**Review**	**1.1**	Ryan Murray (Apr 5, 2024 09:32 PDT) **Ryan Murray, Deputy Director of Arizona Department of Homeland Security & Interim State Chief Information Security Officer**