ARIZONA STATEWIDE SECURITY STANDARD	STATEWIDE STANDARD	State of Arizona

Standard 8340: Identification and Authentication

DOCUMENT NUMBER:	**S8340**
EFFECTIVE DATE:	**May 26, 2021**
REV:	**3.0**

1. AUTHORITY

The authority for this standard is based on Arizona Revised Statutes (A.R.S.) 41-3504: Powers and duties of the department. The Arizona Department of Administration (ADOA) develops, implements, and maintains a coordinated statewide plan for information technology. This includes adopting statewide technical, coordination and security standards for information technology. A.R.S. § 18-104 and § 18-105.

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 – The standard applies to all state information systems. Categorization of systems is defined within the Information Security Program Policy.

- **a. (P)** Policy statements preceded by "(P)" are required for state information systems categorized as Protected.

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

4. EXCEPTIONS

None.

5. ROLES AND RESPONSIBILITIES

Refer to associated Policy (P8340 – Identification and Authentication Policy).

6. STATEWIDE POLICY

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]

6.1.1 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]

c. The content of these temporary passwords shall not be reused; [NIST 800-63B]

d. Salted Hash – The system shall 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

e. 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]
Enforces password maximum lifetime restrictions	● 90 days maximum [PCI DSS 8.2.4] ● 60 days maximum for Administrator and Privilege Accounts [IRS Pub 1075]
Enforces password minimum lifetime restrictions	● 1 day minimum [IRS Pub 1075] ● (P-FTI) -15 day minimum
Prohibits password reuse	● Twenty Four (24) generations [IRS Pub 1075]

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

Password Authentication Parameter	Setting Requirement
Enforce minimum password complexity	● If chosen by user: Eight (8) characters
	● If chosen by the system using a random bit generator: Six (6) characters – may be entirely numeric ● Does not appear in blacklist of commonly-used, expected, or compromised passwords ● No other complexity requirements
Permitted characters and length	● Up to 64 characters in length ● Acceptable characters (ACSII and Unicode) shall include all printable characters including the space character
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 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

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

8. REFERENCES

NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management, National Institute of Standards and Technology, U.S. Department of Commerce, June 2017.

9. ATTACHMENTS

NONE

10. REVISION HISTORY

Date	Change	Revision	Signature
5/26/21	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer** Tim Roemer Tim Roemer (May 25, 2021 22:08 PDT)