

<p>ARIZONA STATEWIDE SECURITY STANDARD</p>	<p>STATEWIDE STANDARD</p>	 <p>State of Arizona</p>
---	--------------------------------------	---

Standard: Identification and Authentication

DOCUMENT NUMBER:	S8340
EFFECTIVE DATE:	JULY 1, 2015
REV:	DRAFT

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. § 41-3504, A.R.S. § 41-3507.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

- 3.1.1 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. § 41-3501(2).**
- 3.1.2 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. Stores and transmits only encrypted representation of passwords; and
- b. Allows the use of a temporary password, unique to each user, for system logons with an immediate change after first use to a permanent password; and [PCI DSS 8.5.3]
- c. The following password authentication parameter settings:

Password Authentication Parameter	Setting Requirement
Enforce minimum password complexity	<ul style="list-style-type: none"> • Six (6) to Eight (8) characters, • Contain both numeric, alphabetic characters, and/or a number,

	<ul style="list-style-type: none"> and special character • Mix of upper-case letters, lower-case letters, numbers, and special characters]; [PCI DSS 8.5.10, 8.5.11] [IRS Pub 1075]
Enforces password maximum lifetime restrictions	<ul style="list-style-type: none"> • 90 days maximum [PCI DSS 8.4] • (P-FTI) - 60 days maximum [IRS Pub 1075]
Enforces password minimum lifetime restrictions	<ul style="list-style-type: none"> • 1 day minimum [PCI DSS 8.4] • (P-FTI) -15 day minimum [IRS Pub 175]
Prohibits password reuse	<ul style="list-style-type: none"> • Six (6) generations [PCI DSS 8.5.12] [IRS Pub 1075]

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

NONE

9. ATTACHMENTS

NONE