ARIZONA STATEWIDE INFORMATION SECURITY	**STATEWIDE POLICY**	**State of Arizona**

STATEWIDE POLICY (8340): IDENTIFICATION AND AUTHENTICATION

DOCUMENT NUMBER:	**(P8340)**
EFFECTIVE DATE:	**DRAFT SEPTEMBER 17, 2018**
REVISION:	**2.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK 8340 IDENTIFICATION AND AUTHENTICATION.

2. PURPOSE

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

- **a.** (P) Policy statements preceded by "(P)" are required for agency information systems categorized as Protected.
- **b.** (P-PCI)Policy statements preceded by "(P-PCI)" are required for agency information systems with payment card industry data (e.g., cardholder data).
- **c.** (P-PHI) Policy statements preceded by "(P-PHI)" are required for agency information systems with protected healthcare information.
- **d.** (P-FTI) Policy statements preceded by "(P-FTI)" are required for agency information 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 IT 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 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of IT PSPs throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology 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 State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Agency Information Technology 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 information systems and assets.

5.4 BU Chief Information Officer (CIO) shall:

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

b. Ensure Identification and Authentication Policy is periodically reviewed and updated to reflect changes in requirements

5.5 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 Technology 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 information systems.

5.6 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.

5.7 System Users of agency information 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 information systems.

6. STATEWIDE POLICY

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

6.1.1 **Network Access to Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for network access to privileged accounts. [NIST 800 53 IA-2(1)]

6.1.2 (P) **Network Access to Non-Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for non-privileged accounts. [NIST 800 53 IA-2(2)] [IRS Pub 1075]

6.1.3 (P) **Local Access to Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for local access to privileged accounts. [NIST 800 53 IA-2(3)] [IRS Pub 1075]

6.1.4 (P) **Network Access to Privileged Accounts – Replay Resistant** - The BU shall ensure the agency information system implements replay-resistant authentication mechanisms for network access to privileged accounts. [NIST 800 53 IA-2(8)] [IRS Pub 1075]

6.1.5 (P) **Remote Access to Privileged Accounts – Separate Device** - The BU shall ensure the agency information system implements multifactor authentication for remote access to privileged 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(11)] [PCI DSS 8.3, 8.3.1] [IRS Pub 1075]

6.1.6 (P) **Remote Access to Non-Privileged Accounts – Separate Device** - The BU shall ensure the agency information system implements multifactor authentication for remote access to non-privileged 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(12)] [IRS Pub 1075] [PCI DSS 8.3.2]

6.2 (P) **Device Identification and Authentication** - The BU shall ensure the agency information 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 information 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, 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 one year; and

f. Disabling the identifier after 90 days of inactivity. [PCI DSS 8.1.4]

6.4 Authenticator Management - The BU shall manage the agency information 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, or device receiving the authenticator; [PCI DSS 8.2.2]

b. Establishing initial authenticator content for authenticators defined by the BU (e.g. password policy);

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/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to agency information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [BU-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI certificates, and key cards)];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; [PCI DSS 8.6]

j. Changing authenticators for role accounts when membership to those accounts changes; and

k. 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 information 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, 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) **PKI-based Authentication** - The BU shall ensure the agency information system, for PKI-based authentication: [NIST 800 53 IA-5(2)] [IRS Pub 1075]

b. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

c. Enforces authorized access to the corresponding private key;

d. Maps the authenticated identity to the account of the individual or group; and

e. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information using the network.

6.4.3 (P) **In Person or Trusted Third-Party Registration** - The BU shall require that the registration process to receive authenticators be conducted in person or by a trusted third-party before the registration authority with authorization by BU-defined personnel or roles. [NIST 800 53 IA-5(3)] [IRS Pub 1075]

6.4.4 Hardware Token-based Authentication - The BU shall ensure the agency information system, for hardware token-based authentication, employs mechanisms that satisfy BU-defined token quality requirements (e.g., compliant with a particular PKI). [NIST 800 53 IA-5(11)]

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

6.6 Cryptographic Module Authentication - The BU shall ensure the agency information 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 information 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 Third-Party Credentials** - The BU shall ensure the agency information system accepts FICAM-approved third-party credentials. [NIST 800 53 IA-8(2)]

6.7.2 **Use of FICAM-Approved Products** - The BU shall employ only FICAM-approved agency information system components in agency information systems to accept third-party credentials. [NIST 800 53 IA-8(3)]

6.7.3 **Use of FICAM-Issued Profiles** - The BU shall ensure the agency information system conforms to FICAM-issued implementation profiles. [NIST 800 53 IA-8(4)]

6.8 (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 website.

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 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

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, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

9/01/2014 **10/11/2016**	Initial Release Updated all Statutes	Draft 1.0	Aaron Sandeen Arizona State CIO Morgan Reed Arizona State CIO
9/17,2018	Updated for PCI-DSS 3.2.1		Morgan Reed, State of Arizona CIO and Deputy Director