TITLE	POLICY NUMBER	
Identification and Authorization Policy	DCS 05-8340	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4.1

I. POLICY STATEMENT

The purpose of this policy is to define the security requirements for establishing and maintaining user accounts for DCS information systems. This Policy will be reviewed annually.

II. APPLICABILITY

This policy applies to all DCS information systems, processes, operations and personnel including employees, contractors, interns, volunteers, external partners and their respective programs and operations.

III. AUTHORITY

A.R.S. § 18-104 Powers and duties of the department; violation; classification

A.R.S. § 41-4282 Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure

HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, November 2022

NIST 800-53 Rev. 5, Recommended Security Controls for Federal Information Systems and Organizations, Sept 2020

IV. EXCEPTIONS

Exceptions to this and all DCS IT policies are approved at the sole discretion of the DCS CIO, will be signed and made an attachment to each applicable policy.

Exceptions to the Statewide Policy Framework taken by DCS shall be documented in the following format:

Section Number	**Exception**	**Explanation / Basis**

V. ROLES AND RESPONSIBILITIES

A. The DCS Director shall:

1. be responsible for the correct and thorough completion of DCS Information Technology Policies, Standards and Procedures (PSPs);

2. ensure compliance with DCS IT PSPs, and;

3. promote efforts within DCS to establish and maintain effective use of DCS information systems and assets.

B. The DCS Chief Information Officer (CIO) shall:

1. work with the DCS Director to ensure the correct and thorough completion of DCS IT PSPs; and

2. ensure DCS PSPs are periodically reviewed and updated to reflect changes in requirements.

C. The DCS Chief Information Security Officer (CISO) shall:

1. advise the DCS CIO on the completeness and adequacy of the DCS activities and documentation provided to ensure compliance with DCS IT PSPs;

2. ensure the development and implementation of adequate controls

enforcing DCS IT PSPs; and

3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems.

D. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on this and all DCS IT PSPs; and

2. monitor employee activities to ensure compliance.

E. System users of DCS information systems shall:

1. become familiar with and adhere to all DCS IT PSPs; and

2. adhere to PSPs regarding the establishment and maintenance of user accounts for agency information systems.

VI. POLICY

A. Identification and Authorization of Organizational Users

DCS information systems shall uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users) [NIST 800 53 IA-2] [HIPAA 164.312 (a)(2)(i), (d)]. DCS shall:

1. ensure DCS information systems implement multifactor authentication for network access to privileged accounts [NIST 800 53 IA-2(1)];

2. ensure DCS information systems implement multifactor authentication for non-privileged accounts [NIST 800 53 IA-2(2)];

3. ensure DCS information systems implement multifactor authentication for local access to privileged accounts [NIST 800 53 IA-2(3)];

4. ensure DCS information systems implement replay-resistant authentication mechanisms for network access to privileged accounts [NIST 800 53 IA-2(8)];

5. ensure DCS information systems implement 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 DCS cryptographic standards for strength of mechanism [NIST 800 53 IA-2(11)].

B. Device Identification and Authentication

DCS information systems shall uniquely identify and authenticate before establishing a local, remote, or network connection [NIST 800 53 IA-3] [PCI DSS 8.1] [HIPAA 164.312 (d)].

C. Identifier Management

DCS shall manage DCS information system identifiers by [NIST 800 53 IA-4]:

1. ensuring that group, shared, or generic account identifiers and authentication methods are not used;

2. receiving authorization from DCS-defined personnel or roles to assign individual, role, service or device identifier;

3. selecting an identifier that identifies an individual, role, service or device;

4. assigning the identifier to the intended individual, role, service or device;

5. preventing reuse of identifiers for one year; and

6. disabling the identifier after 90 days of inactivity.

D. Authenticator Management

DCS shall manage DCS 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)]:

1. verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service or device receiving the authenticator;

2. establishing initial authenticator content for authenticators defined by DCS (e.g. password standard);

3. ensuring that authenticators have sufficient strength of mechanism for their intended use;

4. establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

5. changing default (vendor provided) content of authenticators prior to DCS information systems installation;

6. changing/refreshing authenticators DCS-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI (public key infrastructure) certificates, and key cards) or when a suspected compromise occurs;

7. protecting authenticator content from unauthorized disclosure and modification;

8. requiring individuals to take, and having devices implement, specific controls to protect authenticators;

9. changing authenticators for group role accounts when membership to those account changes; and

10. employing at least one of the following methods to authenticate all users:

    a. password-based authentication;

    b. PKI-based authentication;

    c. in-person or trusted third party registration;

    d. hardware token-based authentication;

    e. multi-factor authentication.

For password-based authentication, the DCS information system shall enforce password controls consistent with this policy [NIST 800 53 IA-5(1)].

For PKI-based authentication [NIST 800 53 IA-5(2)], the DCS information system shall:

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

b. enforce authorized access to the corresponding private key;

c. map the authenticated identity to the account of the individual or group; and

d. implement a local cache of revocation data to support path discovery and validation.

E. Authenticator Feedback

DCS information systems shall obscure feedback of authentication information during the authentication process to protect information from possible exploitation/use by unauthorized individuals [NIST 800 53 IA-6].

F. Cryptographic Module Authentication

DCS information systems shall implement mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication [NIST 800 53 IA-7].

G. Identification and Authentication (Non-Organizational Users)

DCS information systems shall identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) [NIST 800 53 IA-8] [HIPAA 164.312 (a)(2)(i), (d)]. DCS shall:

1. ensure DCS information systems accept only external authenticators that are NIST-compliant; and document and maintain a list of accepted external authenticators [NIST 800 53 IA-8(2)];

2. ensure DCS information system conforms to DCS-defined identity management profiles [NIST 800 53 IA-8(4)].

H. Re-Authentication

DCS shall ensure the agency system requires users to re-authenticate when the following circumstances or situations requiring re-authentication occur:

1. change in role, authenticators, or credentials;

2. execution of DCS-defined privileged functions; or

3. after a DCS-defined period of time.

I. Identity Proofing

DCS 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; and collect, validate, and verify identity evidence. [NIST 800 52 IA-12]

1. DCS shall require evidence of individual identification be presented to the registration authority. [NIST 800 53 IA-12(2)]

2. DCS shall require that the presented identity evidence be validated and verified through DCS-defined methods of validation and verification. [NIST 800 53 IA-12(3)]

3. DCS 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)]

J. Development of Operational Procedures

DCS 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:

1. guidance on selecting strong authentication credentials;

2. guidance for how users should protect their authentication credentials;

3. instructions not to reuse previously used passwords;

4. instructions to change passwords if there is any suspicion the password could be compromised.

VII. DEFINITIONS

Refer to the Policy, Standards and Procedures Glossary located on the Arizona Strategic Enterprise Technology (ASET) website.

VIII. ATTACHMENTS

None.

IX. REVISION HISTORY

Date	Change	Revision	Signature
02 July 2018	Initial Release	1	DeAnn Seneff
08 Jul 2020	Annual update	2	DeAnn Seneff
22 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-17 Identification and Authentication Policy to DCS-05-8340 Identification and Authentication Policy for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	Robert Navarro
07 Mar 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	

05 Aug 2024	Removed references to "unique individual" requirement in VI.G and VI.I per CIO request	4.1	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 8/5/2024 Frank Sweeney AZDCS Chief Information Officer