**ARIZONA DEPARTMENT OF CHILD SAFETY**

| TITLE | | POLICY NUMBER | |
|---|---|---|---|
| Personnel Security Policy | | DCS 05-8270 | |
| RESPONSIBLE AREA | | EFFECTIVE DATE | REVISION |
| DCS Information Technology | | May 20, 2025 | 5 |

## I.    POLICY STATEMENT

The purpose of this policy is to increase the ability of DCS to protect DCS information systems and assets containing sensitive data through personnel security controls. 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 Security and Privacy Controls for Information Systems and Organizations, September 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 IT Policies, Standards, and Procedures (PSPs);

2.    ensure compliance with the DCS PSPs;

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 agency DCS IT PSPs;

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 DCS activities and documentation provided to ensure compliance with DCS IT PSPs;

2.    ensure the development and implementation of adequate controls enforcing the Personnel Security Policy for DCS;

3. ensure all DCS personnel understand their responsibilities with respect to the protection of agency information systems and assets through personnel security controls.

D. Supervisors of DCS employees and contractors shall:

 1. ensure users are appropriately trained and educated on Personnel Security policies;

 2. monitor employee activities to ensure compliance.

E. System Users of DCS information systems shall:

 1. familiarize themselves with this policy and related PSPs;

 2. adhere to DCS PSPs regarding the protection of agency information systems and assets through personnel security controls.

## VI. POLICY

A. Position Categorization

DCS shall:

 1. assign a sensitivity designation (e.g., sensitive or non-sensitive) to all positions;

 2. establish screening criteria for individuals filling those positions; and

 3. review and revise position sensitivity designations annually. Sensitivity designations are based on the individual's exposure to sensitive system information and/or administrative privileges to DCS information systems. Examples of sensitive positions include [NIST 800-53 PS-2]:

  a. Firewall Administrator;

  b. members of the incident response team; and

  c. those with vulnerability scanning duties.

B. Position Definition [HIPAA 164.308 (a)(3)(ii)(A), (a)(3)(ii)(B) - Addressable] [NIST 800-53 PS-9]

DCS shall define information security and privacy responsibilities for all

personnel, including the following:

1. individual or team responsible for establishing, documenting, and distributing security and privacy policies and procedures;

2. individual or team responsible for monitoring and analyzing security and privacy alerts and information, and distributing to appropriate employees and contractors;

3. individual or team responsible for establishing, documenting, and distributing security and privacy incident response and escalation procedures to ensure timely and effective handling of all situations;

4. individual or team responsible for administering user accounts, including additions, deletions, and modifications;

5. individual or team responsible for monitoring and controlling all access to data.

C. Personnel Screening [NIST 800-53 PS-3]

DCS shall screen individuals holding positions designated as sensitive prior to hiring or contracting and rescreen individuals every five (5) years.

D. Personnel Separation [NIST 800-53 PS-4] [HIPAA 164.308 (a)(3)(ii)(C)]

Upon separation of individual employment, DCS shall:

1. disable DCS information system access before the individual is terminated to prevent the individual from having continued access to DCS systems following termination. Terminations should be carefully coordinated with supervisors, human resources and the DCS Help Desk to ensure confidentiality and safety for all involved;

2. Terminate or revoke any authenticators and credentials associated with the individual;

3. conduct exit interviews, if employee is available for interview;

4. retrieve all security-related DCS information system-related property;

5. retain access to DCS information system accounts formerly controlled by separated individual; and

      6.      allow the separated individual access to authorized services such as benefits, reimbursement, and retirement information, according to DCS or State policies.

E.      Personnel Transfer [NIST 800-53 PS-5]

DCS shall:

1.      review logical and physical access authorization to DCS information systems/facilities when personnel are reassigned or transferred to other positions within the organization;

2.      initiates returning old and reissuing new keys, identification cards, and building passes within 24 hours;

3.      close previous information system accounts and establish new accounts and changes DCS system access authorizations;

4.      provide access to official records to which the employee had access at the previous work location and in the previous DCS information system accounts within 24 hours of receiving notification; and

5.      DCS may extend limited access for special purposes on an exception basis.

F.      Access Agreements [NIST 800-53 PS-6]

DCS shall:

1.      Develop and document access agreements for DCS systems;

2.      Review and update the access agreements annually;

3.      Verify that individuals requiring access to DCS information and systems:

      a.      Sign appropriate access agreements prior to being granted access; and

      b.      Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or annually.

G.      Third Party Personnel Security [NIST 800-53 PS-7] [HIPAA 164.314(a)(1)]

DCS shall:

1.     establish personnel security requirements including security roles and responsibilities for external providers;

2.     require external providers to comply with personnel security policies and procedures established by DCS;

3.     document personnel security requirements;

4.     require external providers to notify DCS-defined personnel of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within 24 hours; and

5.     monitor provider compliance.

H.     Third Part Contracts [HIPAA 164.314(a)(2)(i)]

DCS shall ensure that third party contractors specify that the third party will:

1.     comply with the applicable security requirements;

2.     ensure that any subcontractors that create, receive, maintain, or transmit confidential information on behalf of the third-party agree to comply with applicable requirements; and

3.     report to DCS any security incident of which it becomes aware, including breaches of unsecured sensitive information.

I.     Personnel Sanctions [NIST 800-53 PS-8] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]

DCS shall employ a formal sanctions process for individuals failing to comply with established DCS information security and privacy PSPs and document the sanctions applied.

J.     Added Position Description

DCS shall require incorporation of security and privacy roles and responsibilities into organizational position descriptions [NIST 800-53 PS-9].

## VII.   DEFINITIONS

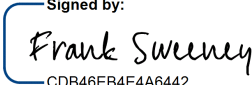Refer to the Policy, Standards and Procedures Glossary located on the Arizona Strategic

Enterprise Technology (ASET) website.

## VIII.   ATTACHMENTS

None.

## IX.   REVISION HISTORY

| Date | Change | Revision | Signature |
|------|--------|----------|-----------|
| **02 Jul 2018** | Initial Release | 1 | DeAnn Seneff |
| **29 Dec 2021** | Annual Review | 2 | Matt Grant |
| **29 Mar 2023** | Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-12 to DCS 05-8270 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 | DocuSigned by:<br>*Frank Sweeney*<br>CDB46EB4E4A6442...<br><br>3/13/2024<br><br>Frank Sweeney<br><br>Chief Information Officer<br><br>AZDCS |

| 20 May 2025 | Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions | 5 | Signed by:<br><br>*Frank Sweeney*<br>CDB46EB4E4A6442...<br><br>5/20/2025<br><br>Frank Sweeney<br><br>Chief Information Officer<br><br>AZDCS |