



|                            |                |          |
|----------------------------|----------------|----------|
| TITLE                      | POLICY NUMBER  |          |
| Data Classification Policy | DCS 05-8110    |          |
| RESPONSIBLE AREA           | EFFECTIVE DATE | REVISION |
| DCS Information Technology | May 20, 2025   | 6        |

## I. POLICY STATEMENT

The purpose of this policy is to provide a framework for the protection of data that is created, stored, processed or transmitted within DCS. The classification of data is the foundation for the specification of policies, procedures, and controls necessary for the protection of Confidential Data. 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:

| <b>Section Number</b> | <b>Exception</b> | <b>Explanation / Basis</b> |
|-----------------------|------------------|----------------------------|
|                       |                  |                            |
|                       |                  |                            |
|                       |                  |                            |
|                       |                  |                            |

#### **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 DCS IT PSPs;
3. promote efforts within DCS to establish and maintain effective use of DCS information systems and assets;
4. be the owner for all Confidential Data sets or shall delegate a data owner for each set of Confidential Data.

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;
2. ensure DCS IT 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 DCS IT PSPs;
  3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems, including classification of data and handling.
- D. DCS Data Owner shall:
1. assign classification of data;
  2. assign data custodians and ensure data custodian is familiar with the protection requirements for Confidential Data;
  3. participate in establishing, approving, and maintaining policies for the protection of data within DCS;
  4. promote data resource management within DCS.
- E. DCS Data Custodian shall:
1. ensure implementation of controls according to DCS IT PSPs.
- F. Supervisors of DCS employees and contractors shall:
1. ensure users are appropriately trained and educated on this and all DCS IT PSPs;
  2. monitor employee activities to ensure compliance.
- G. System Users of DCS information systems shall:
1. become familiar with and adhere to all DCS IT PSPs.

## **VI. POLICY**

- A. Data Classification

Data created, stored, processed or transmitted on DCS information systems shall be classified according to the impact to the state or citizens resulting from the disclosure, modification, breach, or destruction of the data.

**B. Data Classification Categories**

All DCS data shall be classified as one of the following categories [National Institute of Standards and Technology Special Publication (NIST SP) 800-53 RA-2]:

1. Confidential Data – data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements. Examples of Confidential Data include (but are not limited to):
  - a. System Security Parameters and Vulnerabilities, including:
    - i. system security vulnerabilities;
    - ii. generated security information;
    - iii. information regarding current deployment, configuration, or operation of security products or controls.
  - b. Health Information (Confidential), including:
    - i. protected health information [Health Insurance Portability and Accountability Act (HIPAA) - PL 104-191, Sections 261 - 264, 45 CFR Part 160 and 164];
    - ii. medical records [A.R.S. 12-2291, A.R.S. § 12-2292, A.R.S. 36- 445.04, A.R.S. § 36-404, A.R.S. § 36-509, A.R.S. § 36-3805];
    - iii. child immunization data [A.R.S. § 36-135];
    - iv. chronic disease information [A.R.S. § 36-133];
    - v. communicable disease information [A.R.S. § 36-664, A.R.S. § 36- 666];
    - vi. developmental disabilities service records [A.R.S. § 36-68.01, A.R.S. § 36-568.02];
    - vii. emergency medical service patient records [A.R.S. § 36-

- 2220];
- viii. genetic testing records [A.R.S. § 12-2801, A.R.S. § 12-2802];
- ix. home health service records [A.R.S. § 36-160];
- x. midwifery patient records [A.R.S. § 36-756.01];
- xi. state trauma registry [A.R.S. § 36-2221];
- xii. tuberculosis control court hearing information [A.R.S. §36-727];
- xiii. vital records [A.R.S. § 36-342].
- c. Financial Account Data, including:
  - i. credit card, charge card or debit card numbers, retirement account numbers, savings, checking or securities entitlement account numbers [A.R.S. § 44-1373].
- d. Criminal Justice Information, including:
  - i. Child Protective Services records [A.R.S. § 41-1959 (A)]. Any data named within this policy within or attached to assessments and investigations is confidential to the level named in the policy. All notes and narratives are considered to be confidential as the content is variable and may contain various types of sensitive data;
  - ii. any record identifier which has been publicly communicated;
  - iii. criminal history record information [A.R.S. § 41-619.54];
  - iv. criminal justice information [A.R.S. § 41-1750];
- e. Critical Infrastructure/Fuel Facility Reports [A.R.S. § 41-4273].
- f. Eligible Persons (e.g. public officials and their families) [A.R.S. §39-123, A.R.S. § 39-124] See A.R.S. for full definition of Eligible Persons.

- g. Risk Assessment and State Audit Records, including:
  - i. Auditor General Records [A.R.S. § 41-1279.05];
  - ii. Federal risk assessments of infrastructure [A.R.S. § 39-126].
- h. Personally Identifiable Information (except as determined to be public record) [A.R.S. § 18-522, 18-551], including:
  - i. educational records [Family Educational Rights and Privacy Act (FERPA)];
  - ii. social security number [A.R.S. § 44-1373] (Confidential);
  - iii. named identifiers [Health Insurance Portability and Accountability Act (HIPAA) - PL 104-191, Sections 261 - 264, 45 CFR Part 160 and 164];
  - iv. employer names.
- i. Taxpayer Information – Federal Tax Information (FTI) [A.R.S. § 42-2001] [Internal Revenue Service Publication 1075 (IRS Pub 1075)].
- j. Controlled Unclassified Information (CUI) (EO 13556)
- k. Licensing, Certification, Statistics and Investigation Information (of a sensitive nature), including:
  - i. abortion reports [A.R.S. § 36-2161];
  - ii. child death records [A.R.S. § 36-3503];
  - iii. controlled substance records [A.R.S. § 36-2523];
  - iv. emergency medical service investigation records [A.R.S. § 36-2220];
  - v. employment discrimination information [A.R.S. § 41-1482];
  - vi. Health Care Cost Containment Records [A.R.S. § 36-2917];

- vii. Health Care Directives Registry Information [A.R.S. § 36-3295];
  - viii. health care entity licensing information [A.R.S. § 36-2403, A.R.S. § 36-404];
  - ix. medical marijuana records [A.R.S. § 36-2810];
  - x. medical practice review [A.R.S. § 36-445, A.R.S. § 36-445.01];
  - xi. nursing home certification records [A.R.S. § 36-446.10];
  - xii. prescription information [A.R.S. § 36-2604].
- l. Other State-owned Confidential Data, including but not limited to:
    - i. archaeological discoveries [A.R.S. § 39-125];
    - ii. Attorney General opinions [A.R.S. § 38-507];
    - iii. tax examination guidelines [A.R.S. § 42-2001];
    - iv. unclaimed property reports [A.R.S. § 44-315];
    - v. vehicle information [A.R.S. § 41-3452].
  - m. Other Non-state-owned Confidential Data, including but not limited to:
    - i. attorney-client privileged information [A.R.S. § 12-2234];
    - ii. bank records [A.R.S. § 6-129];
    - iii. trade secrets and proprietary information [Intellectual Property laws];
    - iv. management and support information.
  - n. Other records protected by law.
- 2. Public Data – in accordance with Arizona public record’s law, data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

### C. Identification

All data shall be identified as one of the following data classifications:

1. Confidential data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements. Confidential data carries three levels of security;
2. Public; or
3. Data without clear classification markings is assumed to be confidential until otherwise determined.

D. Collection

Collection shall be limited by:

1. encrypting confidential data;
2. properly disposing, destroying, or deleting data;
3. limiting access to confidential information;
4. securely storing confidential data.

E. Handling

1. Need to Know – all Confidential Data shall only be given to those persons that have authorized access and a need to know the information in the performance of their duties [HIPAA 164.308 (a)(3)(ii)(A) – Addressable].
2. Hand Carry – all Confidential Data being hand-carried shall be kept with the individual and protected from unauthorized disclosure.
3. Accounting – for bulk transfer of Confidential Data containing 500 or more records, the receipt and delivery of all Confidential Data shall be monitored and accounted for to ensure the data is not lost and potentially compromised.
4. Guardian – when outside of controlled areas all Confidential Data shall not be left unattended, even temporarily. All Confidential Data shall remain either in a controlled environment or in the employee's physical control at all times. Mail, courier, or other mail services are considered controlled areas.



5. Out of Sight – all Confidential Data shall be turned over or put out of sight when visitors not authorized to view data are present.
6. Conversations – Confidential data shall not be discussed outside of controlled areas when visitors not authorized to hear Confidential Data are present.
7. Movement – unauthorized movement of Confidential Data from controlled areas shall be prohibited [HIPAA 164.310 (d)(1)].

F. Transmission

1. Encryption – any external transmission of Confidential Data shall be encrypted either through link or end-to-end encryption [HIPAA 164.308 (e)(2)(ii) – Addressable].
2. Encryption Strength – encryption algorithm and key length shall be compliant with current state DCS minimum encryption standards as stated in the DCS Policy DCS-05-8350 System and Communications Protection Policy.

G. Processing

Approved Processing - Confidential Data shall only be processed on approved devices.

H. Media Protection

Confidential Data Protection - all Confidential Data shall be protected and implemented at minimum controls as stated in applicable DCS-05-8250 Media Protection Policy [HIPAA 164.310 (d)(2)].

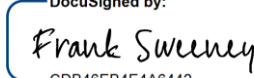
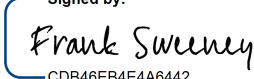
## VII. DEFINITIONS

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

## VIII. ATTACHMENTS

None.

**IX. REVISION HISTORY**

| <b>Date</b>         | <b>Change</b>  | <b>Revision</b> | <b>Signature</b>  |
|---------------------|--|-----------------|---|
| <b>02 July 2018</b> | Initial Release  | 1               | DeAnn Seneff  |
| <b>10 Apr 2019</b>  | Name change  | 2               | DeAnn Seneff  |
| <b>7 Jul 2019</b>   | Annual Review  | 3               | DeAnn Seneff  |
| <b>28 Mar 2023</b>  | Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-03 to DCS 05-8110 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers. | 4               | Robert Navarro  |
| <b>07 Mar 2024</b>  | Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions  | 5               | <p>DocuSigned by:</p>  <p>CDB46EB4E4A6442...</p> <p>3/13/2024</p> <p>Frank Sweeney</p> <p>Chief Information Officer</p> <p>AZDCS</p> |
| <b>20 May 2025</b>  | Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions  | 6               | <p>Signed by:</p>  <p>CDB46EB4E4A6442...</p> <p>5/28/2025</p> <p>Frank Sweeney</p> <p>Chief Information Officer</p> <p>AZDCS</p>    |