



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
System Privacy Policy	DCS 05-8410	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	August 15, 2023	3

I. POLICY STATEMENT

The purpose of this policy is to provide more detailed guidance for the development of a system privacy notice based on standards, regulations, and best practices.

II. APPLICABILITY

This policy applies to all DCS information systems, processes, operations, and personnel to include all 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 Policies, Standards, and Procedures (PSPs);
2. ensure compliance with 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 DCS IT PSPs;
2. ensure DCS PSPs are periodically reviewed and updated to reflect changes in requirements.

C. The DCS Information Security Officer (ISO) 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 PSPs;
3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems;

4. request changes and/or exceptions to existing PSPs from the State CISO;
5. ensure all personnel understand their responsibilities with respect to privacy of Confidential data.

D. The DCS Privacy Officer shall:

1. advise the State CISO and the State CPO on the completeness and adequacy of the DCS activities and documentation provided to ensure compliance with privacy laws, regulations, statutes and Statewide IT Privacy PSPs throughout DCS;
2. assist the Department to ensure the privacy of sensitive personal information within DCS's possession;
3. review and approve DCS privacy PSPs and requested exceptions from the statewide privacy PSPs;
4. identify and convey to the DCS CIO the privacy risk to DCS information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

E. Data users and owners of DCS privacy-related data shall:

1. Become familiar with and adhere to all DCS PSPs.

F. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on this and all DCS 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 PSPs;
2. adhere to PSPs regarding system privacy.

VI. POLICY

A. Authority to Collect

DCS shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or DCS information system need. For additional specificity on the authority to collect, refer to DCS-05-8330, System Security Audit. [NIST 800 53 AP-1] [Privacy Acts] [HIPAA 164.520(a)(1)].

B. Purpose Specification

DCS shall describe the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices [NIST 800 53 AP-2] [HIPAA 164.520(a)(1)] [A.R.S. § 41-4152].

C. Access Enforcement

DCS shall ensure the DCS information system enforces approved authorizations for logical access to PII in accordance with applicable control policies (e.g., identity-based policies, role-based policies) [NIST 800-53 AC-3].

D. Least Privilege

DCS shall employ the concept of least privilege, allowing only authorized accesses to PII for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions [NIST 800-53 AC-6].

E. Governance and Privacy Program [NIST 800 53 AR-1]

DCS shall:

1. appoint a senior DCS official for Privacy accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and DCS information systems [HIPAA 164.530(a)(1)] [EO 2008-10];
2. monitor federal and state privacy laws for changes that affect the privacy program;
3. allocate resources to implement and operate the organization-wide privacy program;
4. develop a strategic organizational privacy plan for implementing

applicable privacy controls, policies, and procedures;

5. develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, DCS information systems, or technologies involving PII;
6. update privacy plan, policies, and procedures annually.

F. Privacy Impact and Risk Assessment [NIST 800 53 AR-2]

DCS shall:

1. document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;
2. conduct Privacy Impact Assessments (PIAs) for DCS information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any existing DCS policies and procedures;
 - a. The DCS PIA will be conducted upon completion of a Privacy Threshold Analysis (PTA) that indicates the requirement of a PIA.
3. ensure PIAs are conducted prior to any new collection of PII or upon significant changes in the architecture, information flow, or use of PII within existing systems.

G. Privacy Requirements for Contractors and Providers [NIST 800 53 AR3]

DCS shall:

1. establish privacy roles, responsibilities, and access requirements for contractors and service providers;
2. include privacy requirements in contracts and other acquisition-related documents;
3. require users to affirm their understanding of privacy responsibilities which is included in the mandatory user's annual training.
 - a. Each user will sign the DCS Affirmation Form following privacy training.

H. Privacy Monitoring and Auditing

DCS shall monitor and audit privacy controls and internal privacy policy annually to ensure effective implementations [NIST 800 53 AR-4].

I. Privacy Awareness and Training [NIST 800 53 AR-5]

DCS shall:

1. develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that DCS employees and contractors understand privacy responsibilities and procedures;
2. administer basic privacy training annually and targeted, role-based privacy training for DCS employees and contractors having responsibility for PII or for activities that involve PII annually;
3. inform all individuals responsible for handling consumer inquiries about DCS's privacy practices or DCS's compliance with privacy regulations of all the requirements in these regulations and how to direct consumers to exercise their rights under these regulations;
4. ensure that DCS employees and contractors certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

J. Privacy Reporting

DCS shall conduct an initial evaluation, develop, disseminate, and establish and follow a schedule for regularly updating as necessary, but at least every three years, reports to the State Privacy Officer (SPO) and other appropriate oversight bodies to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance [NIST 800 53 AR-6].

K. Privacy Enhanced System Design and Development

DCS shall design information systems to support privacy by automating privacy controls [NIST 800 53 AR-7].

L. Accounting of Disclosures

DCS, consistent with state privacy acts and subject to any applicable exceptions or exemptions, shall [NIST 800 53 AR-8] [HIPAA 164.528(a)]:

1. keep an accurate accounting of disclosures of information held in each system of records under its control, including:
 - a. date, nature, and purpose of each disclosure record;
 - b. name and address of the person or entity to which the disclosure was made.
2. retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer or as required by law.

3. Data Quality

DCS [NIST 800 53 DL-1] shall:

- a. confirm to the greatest extent possible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
- b. collect PII directly from the individual to the greatest extent possible;
- c. check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems annually;
- d. issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

M. Data Integrity

DCS shall document processes to ensure the integrity of PII through existing security controls [NIST 800 53 DI-2].

N. Minimization of Personally Identifiable Information

DCS [NIST 800 53 DM-1] shall:

1. identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

2. limit the collections and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;
3. limit the use of PII for testing, training, and research when feasible;
4. conduct an initial evaluation of PII holdings and establish and follow a schedule for regularly reviewing those holdings annually and update as necessary to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

O. Data Retention and Disposal

DCS [NIST 800 53 DM-2] shall:

1. retain each collection of PII for a DCS-specified time period to fulfill the purposes identified in the notice or as required by law;
2. dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with an Arizona State Library-approved record retention schedules and in a manner that prevents loss, theft, misuse, or unauthorized access [A.R.S. § 44-7601] [A.R.S. § 41-151.12];
3. use techniques, documented in the Media Protection Policy ([DCS 05-8250](#)) to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

P. Consent

For collection, use, and disclosures of PII not already authorized by law, DCS [NIST 800 53 IP-1] shall:

1. provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection [HIPAA 164.522(a)(1)];
2. provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
3. obtain consent, where feasible and appropriate, from individuals prior to

any new uses or disclosure of previously collected PII;

4. ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Q. Individual Access

Consistent with laws and regulations, and subject to any applicable exceptions or exemptions, DCS [NIST 800 53 IP-2] [HIPAA 164.524(a)] shall:

1. provide individuals the ability to have access to their PII maintained in its system(s) of records;
2. publish rules and regulations governing how individuals may request access to records maintained in a system of records [HIPAA 164.524(b)(c)(d)];
3. adhere to requirements, policies, and guidance for the proper processing of PII requests.

R. Redress [NIST 800 53 IP-3] [HIPAA 164.526(a)-(f)]

For collection, use, and disclosures of PII not already authorized by law DCS [NIST 800 53 IP-3] [HIPAA 164.526(a)-(f)] shall:

1. provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate;
2. establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifying affected individuals.

S. Complaint Management [NIST 800 53 IP-4] [HIPAA 164.530(d)]

For collection, use, and disclosures of PII not already authorized by law, DCS shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about DCS privacy practices [NIST 800 53 IP-4] [HIPAA 164.530(d)].

T. Inventory of PII

DCS [NIST 800 53 SE-1] shall:

1. establish, maintain, and update an inventory that contains a listing of all programs and DCS information systems identified as collecting, using, maintaining, or sharing PII;
2. provide each update of the PII use to DCS CIO, DCS ISO, and the DCS Privacy Officer to support the establishment of information security requirements for all new or modified DCS information systems containing PII annually.

U. Privacy Incident Response

DCS [NIST 800 53 SE-2] shall:

1. develop and implement a Privacy Incident Response Plan consistent with the DCS Incident Response Planning Policy ([DCS 05-8240](#));
2. provide an organized and effective response to privacy incidents in accordance with DCS Privacy Incident Response Plan.

V. Privacy Notice

The following guidance is offered for the development of a Privacy Notice [NIST 800 53 TR-1] [HIPAA 164.520(c)] [A.R.S. § 41-4152]. The Privacy Notice provides effective notice to the public and to individuals by addressing:

1. its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
2. authority for the collection of PII;
3. the choices, if any, individuals may have regarding how DCS uses PII and the consequences of exercising or not exercising those choices;
4. the ability to access and have PII amended or corrected if necessary;
5. descriptions of:
 - a. how DCS collects PII and the purpose(s) for which it collects that information;

- b. how DCS uses PII internally;
 - c. whether DCS shares PII with external entities, the categories of those entities, and the purposes for such sharing;
 - d. whether individuals have the ability to consent to specific uses of sharing of PII and how to exercise any such consent;
 - e. an individual's rights to access/obtain PII;
 - f. how PII will be protected;
 - g. methods to communicate with the DCS Privacy Officer.
6. DCS's obligations to:
- a. revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change;
 - b. provide notice in clear and conspicuous language when individuals are first asked to provide PII to DCS.

W. Dissemination of Privacy Program Information

DCS [NIST 800 53 TR-3] shall:

- 1. ensure the public has access to information about its privacy notice and is able to communicate with the DCS Privacy Officer;
- 2. ensure that its privacy notices are publicly available through DCS websites or publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy notices.

X. Internal Use

DCS shall use PII internally only as authorized by law or for the authorized purpose(s) described in the privacy notice [NIST 800 53 UL-1].

Y. Information Sharing with Third Parties

DCS [NIST 800 53 UL-2] [HIPAA 164.508(a)] shall:

1. only share PII externally as authorized by law, or for the authorized purposes identified and described in the privacy notice or in a manner compatible with those purposes;
2. where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, Service Level Agreements, Business Associate Agreements, Data Sharing Agreements or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used and offer the same level of protection as documented in this policy [HIPAA 164.514(e)(4)];
3. monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized sharing of PII;
4. evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether an additional or new privacy notice is required.

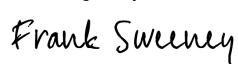
VII. DEFINITIONS

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
8 Jul 2020	Annual Review	2	Matt Grant
15 Aug 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-19 to DCS 05-	3	DocuSigned by:  CDB46EB4E4A6442...

	8410 System Privacy Policy for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.		8/31/2023 Frank Sweeney Chief Information Officer AZDCS