

*Arizona Department of Child Safety*

TITLE	POLICY NUMBER	
System Privacy Policy	DCS 05-8410	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	June 30, 2024	4

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. This Policy will be reviewed annually.

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 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 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. Policy and Procedures - DCS shall [NIST 800 53 PT-1]

1. Develop, document, and disseminate to DCS-defined roles
 - a. A DCS-level PII processing and transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
 - b. Procedures to facilitate the implementation of the PII processing and transparency policy and the associated PII processing and transparency controls;
 2. Designate a DCS-defined official to manage the development, documentation, and dissemination of the PII processing and transparency policy and procedures; and
 3. Review and update the current PII processing and transparency:
 - a. Policy annually and following data breach events; and
 - b. Procedures annually and following data breach events or changes in operations to necessitate procedural changes.
- B. Authority to Collect - DCS shall determine and document the laws, executive orders, directive, regulations, or policies that permit the processing and processing operations (e.g., creation, collection, use, processing, maintenance, dissemination, disclosure, logging, generation, transformation, analysis, and disposal) of PII and restricts processing and processing operations to only that which is authorized. . For additional specificity on the authority to collect, refer to Standard 8330, System Security Audit. [NIST 800 53 PT-2] [Privacy Acts] [HIPAA 164.520(a)(1)]
- C. Purpose Specification - DCS shall: [NIST 800 53 PT-3] [HIPAA 164.520(a)(1)] [ARS 41-4152]
1. Identify and document the purpose(s) for processing personally identifiable information (PII);
 2. Describe the purpose(s) in the public privacy notices and policies of DCS;
 3. Restrict DCS-defined processing of PII data to only that which is compatible with the identified purpose(s); and
 4. Monitor changes in processing PII and implement training, monitoring, and/or auditing mechanisms to ensure that any changes are made in accordance with DCS-defined requirements.

- D. Privacy Program Plan - DCS shall: [NIST 800 53 PM-18]
1. Develop and disseminate a DCS-wide privacy program plan that provides an overview of the DCS privacy program, and;
 - a. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;
 - b. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;
 - c. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
 - d. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
 - e. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
 - f. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the state;
 2. Update the plan annually and to address changes in privacy laws and policy and DCS-changes and problems identified during plan implementation or privacy control assessments.
- E. Privacy Program Leadership Role - DCS shall appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the DCS-wide privacy program. [NIST 800 53 PM-19] [HIPAA 164.530(a)(1)] [EO 2008-10]
- F. Privacy Reporting - DCS shall: [NIST 800 53 PM-27]
1. Develop state privacy officer defined privacy reports and disseminate to the State Privacy Officer (SPO) and other appropriate oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and to senior management and other personnel with responsibility for monitoring privacy program compliance; and

2. Review and update privacy reports as necessary, but at least every three years.
- G. Accounting of Disclosures - DCS, consistent with state privacy acts and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 PM-21] [HIPAA 164.528(a)]
1. Develop and maintain an accurate accounting of disclosures of PII held in each system of records under its control, including:
 - a. Date, nature, and purpose of each disclosure of a record
 - b. Name and address of the person or other contact information of the individual or agency 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. However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to:
[http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20\(IT\).pdf](http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf) Item 10a. and b.; and
 3. Make the accounting of disclosures available to the individual to whom the PII relates upon request.
- H. Personally Identifiable Information Quality Operations - DCS shall check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle annually and correct or delete inaccurate or outdated personally identifiable information. [NIST 800-53 SI-18]
- a. Individual Requests - DCS shall correct or delete personally identifiable information upon request by individuals or their designated representatives. [NIST 800-53 SI-18(4)]
 - b. De-identification - DCS shall remove the DCS-defined elements of personally identifiable information from datasets and evaluate annually for effectiveness of de-identification. [NIST 800-53 SI-19]
 - c. Notice of Correction or Deletion - DCS shall notify DCS-defined recipients of PII and individuals that the PII has been corrected or deleted. [NIST 800-53 SI-18(5)]
2. Personally Identifiable Information Quality Management - DCS shall develop and document DCS-wide policies and procedures for: [NIST 800 53 PM-22] [HIPAA 164.526(a)-(f)]

- a. Reviewing for the accuracy, relevance, timeliness, and completeness of PII across the information life cycle;
 - b. Correcting or deleting inaccurate or outdated PII;
 - c. Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and
 - d. Appeals of adverse decisions on correction or deletion requests.
3. Minimization of Personally Identifiable Information Used in Testing, Training, and Research - DCS shall: [NIST 800 53 PM-25]
 - a. Develop, document, and implement policies and procedures that address the use of PII for internal testing, training, and research:
 - b. Limit or minimize the amount of PII used for internal testing, training, and research; Authorize the use of PII when such information is required for internal testing, training, and research; and
4. Review and update policies and procedures annually. Consent - DCS shall implement State Privacy Officer (SPO) approved tools and mechanisms for individuals consent to the processing of their PII prior to its collection that facilitate individuals' informed decision-making. [NIST 800 53 PT-4]
5. For collection, use, and disclosures of PII not already authorized by law DCS shall 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)]
- I. Dissemination of Privacy Program Information - DCS shall maintain a central resource webpage on the DCS's principal public website that serves as a central source of information about DCS's privacy program and that: [NIST 800 53 PM-20][HIPAA 164.524(a)]
 - i. Ensures that the public has access to information about DCS privacy activities and can communicate with its senior agency official for privacy;
 - ii. Ensures that organizational privacy practices and reports are publicly available; and
 - iii. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

- iv. Publish rules and regulations governing how individuals may request access to records maintained in a system of records; and [HIPAA 164.524(b),(c),(d)]
 - v. Adhere to requirements and policies and guidance for the proper processing of PII requests. [HIPAA 164.524(b),(c),(d)]
 - b. Privacy Notice - DCS shall provide notice to individuals about the processing of PII that: [NIST 800 53 PT-5][HIPAA 164.520(c)] [ARS 41-4152]
 - i. Is available to individuals upon first interacting with an organization, and subsequently at DCS-defined frequency;
 - ii. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;
 - iii. Identifies the authority that authorizes the processing of personally identifiable information;
 - iv. Identifies the purposes for which personally identifiable information is to be processed; and
 - v. Includes DCS-defined information.
 - c. Privacy Policies on Websites, Applications, and Digital Services - DCS shall develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: [NIST 800 53 PM-20(1)]
 - i. Are written in plain language and organized in a way that is easy to understand and navigate;
 - ii. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and
 - iii. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.
 - d. Complaint Management - DCS shall Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: [NIST 800 53 PM-26]

- i. Mechanisms that are easy to use and readily accessible by the public;
 - ii. All information necessary for successfully filing complaints;
 - iii. Tracking mechanisms to ensure all complaints received are reviewed and addressed within a DCS-defined time period not to exceed CPO-defined time period;
 - iv. Acknowledgement of receipt of complaints, concerns, or questions from individuals within DCS-defined time period not to exceed CPO-defined time period; and
 - v. Response to complaints, concerns, or questions from individuals within DCS-defined time period not to exceed CPO-defined time period.
- J. Specific Categories of Personally Identifiable Information - DCS shall apply specific processing conditions as required for specific categories of PII. [NIST 800 53 PT-7].
 - 1. Social Security Numbers - When a system processes Social Security numbers, DCS shall: [NIST 800 53 PT-7(1)]
 - a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;
 - b. Not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and
 - c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.
- K. Dissemination of Privacy Program Information - DCS shall maintain a central resource webpage on the DCS's principle public website that serves as a central source of information about the DCS's privacy program and that: [NIST 800 53 PM-20]
 - 1. Ensures the public has access to information about its privacy notice and is can communicate with its Privacy Officer; and
 - 2. Ensures that DCS privacy practices and reports are publicly available; and

3. Employs publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

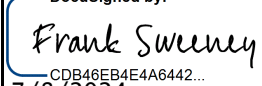
VII. DEFINITIONS

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 05-8410 System Privacy Policy for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.	3	Frank Sweeney AZDCS CIO
30 Jun 2024	Annual review/updates to mirror AZDoHS	4	DocuSigned by:  <small>CDB46EB4E4A6442...</small> 7/8/2024 Frank Sweeney Chief Information Officer AZDCS

