TITLE	POLICY NUMBER	
Policy Administration Policy	DCS 05-8111	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to establish authority for authoring, reviewing, and approving DCS IT policies, procedures, and standards to ensure a safe and secure IT Network environment for DCS customers, and to comply with Federal and State regulations. 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) within DCS;

2. ensure compliance with the Policy Administration Policy;

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 within DCS;

2. ensure the Policy Administration Policy is 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 Policy Administration Policy for DCS.

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 all agency BUs;

2. assist the agency to ensure the privacy of sensitive personal information within DCS's possession;

3. assist with the development, implementation, review, and approval of DCS privacy Policies, Standards, and Procedures (PSPs) related to the Privacy Act to assure that personal information, and requested exceptions, are handled in compliance with statewide privacy PSPs;

4. identify and convey to the DCS CIO the privacy risk to agency information systems and data, based on current implementation of privacy controls and mitigation options to improve privacy;

5. serve as the DCS advisor in consultation with legal relating to public disclosure of information and any identified privacy issues.

E. 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.

F. System users of DCS information systems shall:

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

VI. POLICY

A. The DCS CIO is responsible for the management of all DCS Information Technology Policies, Standards, and Procedures.

1. The DCS CIO is responsible for the enforcement of all DCS IT Policies,

Standards, and Procedures.

2. The DCS CIO or designee are the signing authorities for all DCS Information Technology Policies, Standards, and Procedures.

3. DCS Divisions and Programs may not create or institute DCS Information Technology Policies.

4. Policies will not be written that circumvent or are less stringent than already official DCS Information Technology Policies.

B. DCS IT Standards and Procedures may be initiated by individual subject matter experts within DCS agencies as needs are identified.

1. Final authorization and signing authority for all DCS standards and procedures is the DCS-CIO or designee.

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
06 Dec 2017	Initial Release	1	DeAnn Seneff
02 Jul 2018	Annual update	2	DeAnn Seneff
28 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-01 IT Systems Policies, Standards, and Procedures Policy to DCS-05-8111 Policy Administration Policy for better tracking with Arizona Department	3	Robert Navarro

	Homeland Security (AZDOHS) policy numbers.		
07 Mar 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 3/13/2024 Frank Sweeney Chief Information Officer AZDCS