TITLE	POLICY NUMBER	
Policy Exception Policy	DCS 05-8112	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to establish controls for DCS employees and systems to document exceptions to DCS Information Technology policies. 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 Chief Information Officer (CIO) shall:

1. be ultimately responsible for the correct and thorough completion of Information Technology Policies, Standards and Procedures (PSPs);

2. review and approve DCS PSPs and applicable exceptions.

B. 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 DCS compliance with this and all Information Technology PSPs;

3. promote efforts within DCS to establish and maintain effective use of DCS information systems and assets;

4. work with DCS CIO to ensure the correct and thorough completion of DCS Information Technology PSPs;

5. ensure all DCS policies are periodically reviewed and updated to reflect changes in requirements;

6. ensure the development and implementation of adequate security controls

enforcing all DCS policies;

7. ensure all DCS personnel understand their responsibilities included in DCS policies.

C. 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.

D. System Users of DCS information systems shall:

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

VI. POLICY

A. Information Technology Policy Exceptions

1. Exceptions to IT policy must be properly documented, approved, and retained in a system of record for future regulatory audits and the security of the IT systems.

2. Policy exceptions can only be signed (approved) by the DCS CIO.

a. Based on the possible severity of the impact of an exception, the DCS CIO may request approval of said exception from the DCS Director.

b. Without an exception in place, all IT policies apply to all persons and systems within DCS.

c. DCS divisions, offices, managers, etc. are not authorized to create exceptions to IT policies at any time.

d. Exceptions to policies will be annotated in Section 4 of applicable policies and will be reviewed annually.

e. Requests for exceptions to policies must be sent to the DCS IT Security Office by creating a ticket in the DCS ServiceDesk System.

f. Anyone requiring assistance with this process shall contact the DCS IT Security Office with questions.

B. Information Technology Policy Exception Management

1. All exceptions to IT policy will managed and tracked by the DCS CISO and the DCS Policy Unit.

2. Exceptions to DCS IT PSPs will be treated as confidential information and not published in any manner to the public or DCS as a whole.

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 Review	2	DeAnn Seneff
28 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-02 to DCS 05-8112 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: Frank Sweeney CDB46EB4E4A6442... 3/13/2024 Frank Sweeney Chief Information Officer AZDCS