ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
Contingency Planning Policy	DCS 05-8230	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	May 20, 2025	5

I. POLICY STATEMENT

The purpose of this policy is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability. 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);

2. identify and convey contingency planning needs;

3. ensure compliance with DCS PSPs;

4. 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. assign the necessary resources to document, implement, and maintain the contingency plan, including the following roles:

   a. recommend/ensure continuity plans are documented in the contingency plan;

b. approve developed and modified contingency plans;

c. 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 the Contingency Planning Policy for DCS;

3. ensure all DCS personnel understand their responsibilities with respect to business continuity and disaster recovery planning;

4. work with project leader on security and privacy related issues involving the development, maintenance, or testing of the contingency plan.

D. Information System Owners shall:

1. participate in establishing, approving, and maintaining policies for the protection controls applicable to the agency information systems under their control;

2. work with the project leader on agency information system related issues involving the development, maintenance, or testing of the contingency plan.

E. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on the DCS Contingency Planning Policy;

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;

2. adhere to PSPs regarding the Contingency Planning Policy.

VI. POLICY

A. Developing a Contingency Plan

DCS shall develop a contingency plan [National Institute of Standards and Technology (NIST) 800-53 CP-2] [Health Insurance Portability and Protection Act (HIPAA) 164.308(a)(7)(i), 164.308(a)(7)(ii)(b), 164.308(a)(7)(ii)(c), 164.310(a)(2)(i)] that:

1. identifies essential mission and business functions and the associated contingency requirements consistent with Establishing an Essential Records List published by Arizona State Library, Archives and Public Records;

2. provides recovery objectives, restoration priorities, and metrics;

3. addresses contingency roles, responsibilities, assigned individuals with contact information;

4. addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. addresses eventual, full information systems restoration without deterioration of the security safeguards originally planned and implemented;

6. addresses resumption of essential missions and business functions within a time frame specified by DCS CIO and based on mission needs, applicable regulations, Arizona State Library, Archives and Public Records requirements and applicable contracts and agreements with external DCS organizations. [NIST 800-53 CP-2(3)];

7. identifies critical information system assets supporting organizational missions and business functions; [NIST 800-53 CP-2(8)] [HIPAA 164.308(a)(7)(ii)(E)];

8. includes procedures for obtaining necessary electronic protected health information during an emergency [HIPAA 164.312(a)(2)(ii)].

B. Managing the Contingency Plan

DCS shall:

1. distribute the contingency plan to key contingency personnel and organizational elements;

2. coordinate contingency planning activities with security incident handling activities;

3. review the contingency plan annually;

4. revise the contingency plan to address changes to the organization, DCS information systems, operational environment, or problems encountered during plan implementation, execution, or testing;

5. communicate contingency plan changes to key contingency personnel and organizational elements;

6. protect the contingency plan from unauthorized disclosure and modification.

C. Contingency Planning Coordination

DCS shall coordinate the development of the contingency plan for each DCS information system with organizational elements responsible for related plans [NIST 800-53 CP-2(1)].

D. Contingency Training

DCS shall provide contingency training to DCS information system users consistent with assigned roles and responsibilities before authorizing access, when required by DCS information system changes, and annually thereafter. DCS shall update and review contingency training content annually and following a major incident. [NIST 800-53 CP-3].

E. Test Contingency Plan - DCS shall test the contingency plan for the DCS information system annually to determine the effectiveness of the plan and the organizational readiness to execute the plan, review the contingency plan test results, and initiate corrective action [NIST 800-53 CP-4] [HIPAA 164.308 (a)(7)(ii)(D)].

1. Contingency Test Plan Coordination – DCS shall coordinate contingency plan testing for each DCS information system with organizational elements responsible for related plans [NIST 800-53 CP-4(1)].

F. Alternate Storage Site

DCS shall establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information and

ensure that the alternative storage site provides information security safeguards equivalent to those of the primary storage site [NIST 800-53 CP6].

1. Separation from Primary Storage Site – the alternative storage site shall be separated from the primary storage site to reduce susceptibility to the same hazards [NIST 800-53 CP-6(1)].

2. Accessibility – DCS shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions [NIST 800-53 CP-6(3)].

3. Arizona State Library, Archive and Public Records is an alternative site by statute (A.R.S. 41-151.12).

G. Alternate Processing Site

DCS shall: [NIST 800-53 CP-7]

a. establish an alternate processing site including necessary agreements to permit the transfer and resumption of DCS information system operations for essential missions/business functions with DCS defined time periods consistent with recovery time and recovery point objectives when the primary process capabilities are unavailable;

b. ensure that equipment and supplies to transfer and resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the DCS defined period for transfer/resumption;

c. ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site;

2. Separation from the Primary Site – DCS shall identify an alternative processing site that is separated from the primary site to reduce susceptibility to the same threats [NIST 800-53 CP-7(1)];

3. Accessibility – DCS shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions [NIST 800-53 CP-7(2)];

4. Priority of Service – DCS shall develop alternative processing site agreements that contain priority of service provisions in accordance with the organization's availability requirements [NIST 800-53 CP-7(3)].

H. Alternate Telecommunications Site

DCS shall ensure alternate telecommunications services are established including necessary agreements to permit the resumption of DCS information system operations for essential missions and business functions within DCS defined time period when the primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites [NIST 800- 53 CP-8].

1. Priority of Service Provisions – DCS shall ensure primary and alternate telecommunications service agreements are developed that contain priority-of-service provisions in accordance with DCS's availability requirements, and request telecommunication service priority for all telecommunications services used for national or state security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier [NIST 800-53 CP-8 (1)].

2. Single Points of Failure – DCS shall ensure alternate telecommunications services are obtained, with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunication services [NIST 800-53 CP-8(2)].

I. DCS Information System Backup

DCS shall: [NIST 800-53 CP-9] [HIPAA 164.308(7)(ii)(A)]

a. conduct backups of user-level and system-level information contained in the DCS information system, and DCS information system documentation including security-related documentation within DCS's defined frequency consistent with recovery time and recovery point objectives;

b. protect the confidentiality, integrity, and availability of the backup information at storage locations;

1. Testing for Reliability/Integrity - DCS shall test backup information at least annually to verify media reliability and information integrity. [NIST 800-53 CP-9(1)]

2. Cryptographic Protection - DCS shall implement cryptographic mechanisms to prevent unauthorized disclosure and modification of DCS-defined backup information. [NIST 800-53 CP-9(8)]

J. System Recovery and Reconstitution - DCS shall provide for the recovery and reconstitution of the DCS information system to a known state after a disruption, compromise, or failure [NIST 800-53 CP-10].

1. Transaction Recovery – DCS shall implement DCS information systems to perform transaction recovery for any system that is transaction-based [NIST 800-53 CP-10(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

Date	Change	Revision	Signature
06 Dec 2017	Initial Release	1	DeAnn Seneff
02 Jul 2018	Annual Review	2	DeAnn Seneff
29 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-08 to DCS 05-8230 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
20 May 2025	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	5	Signed by: Frank Sweeney CDB46EB4E4A6442... 5/20/2025 Frank Sweeney Chief Information Officer AZDCS