TITLE	POLICY NUMBER	
Media Protection Policy	DCS 05-8250	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 15, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to increase the ability for DCS to ensure the secure storage, transport, and destruction of sensitive information. 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 IT Policies, Standards, and Procedures (PSPs) within DCS;

2. ensure compliance with the Media Protection Policy;

3. promote efforts within DCS to establish and maintain effective use of agency 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 Media Protection PSPs are periodically reviewed and updated.

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 Media Protection PSPs for DCS;

3. request changes and/or exceptions to existing Media Protection PSPs from the State CISO;

4. ensure all DCS personnel understand their responsibilities with respect to protection of removable media in connection with agency information systems and premises.

D. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on Media Protection policies;

2. monitor employee activities to ensure compliance.

E. System Users of DCS information systems shall:

1. familiarize themselves with this policy and related DCS IT PSPs;

2. adhere to DCS IT PSPs regarding protection of removable media in connection with agency information systems and premises.

VI. POLICY

A. Media Access

DCS shall restrict access to digital and non-digital media to authorized individuals [NIST 800-53 MP-2] [HIPAA 164.308(a)(3)(ii)(A)].

B. Media Marking

DCS shall mark, in accordance with DCS policies and procedures, information system digital and non-digital media containing confidential information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information, as well as exempt removable digital media from marking as long as the exempted items remain within a controlled environment [NIST 800-53 MP-3].

C. Media Storage

DCS shall physically control and securely store digital and non-digital media containing confidential information within controlled areas [NIST 800- 53 MP-4] [ARS 39-101].

D. Media Inventories

DCS shall maintain inventory logs of all digital media containing confidential information and conduct inventories annually.

E. Media Transport

DCS shall protect and control digital and non-digital media containing confidential information during transport outside controlled areas [NIST 800-53 MP-5].

1. Cryptographic Protection – DCS shall employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas. Cryptographic mechanisms must comply with System and Communication Protection Standard S8350 [NIST 800-53 SC-28(1)] [HIPAA 164.312(c)(2)].

2. Media Transport Policies - DCS shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential information into and out of a protected facility, and the movement of these items within the facility [HIPAA 164.310(d)(1)].

3. Secure Delivery – DCS shall send confidential digital and non-digital media by secured courier or other delivery method.

4. Record of Movement – DCS shall maintain a record, including the person(s) responsible, of the movements of hardware and digital media [HIPAA 164.310(d)(2)(iii)].

    a. Data Backup – DCS shall create a retrievable, exact copy of confidential data, when needed before movement of equipment [HIPAA 164.310(d)(2)(iv)].

    b. Backup Storage – DCS shall store digital media backups in a secure location and review the location’s security, at least annually.

5. Management Approval – DCS shall ensure management approves any media that is moved from a controlled area.

6. Media Sanitization – DCS shall sanitize digital and non-digital system media containing confidential information prior to disposal, release of organizational control, or release for reuse using defined sanitization

techniques and procedures in accordance with the Media Protection Standard [NIST 800-53 MP-6] [HIPAA 164.310(d)(2)(i)] [HIPAA 164.310(d)(2)(ii)].

a. Secure Storage – Secure storage containers used for materials that are to be destroyed.

b. Verify Sanitization - DCS shall review, approve, track, document, and verify media sanitization and disposal actions. [NIST 800-53 MP-6(1)]

F. Media Use

DCS shall define restricted devices in the Media Protection Standard of portable storage devices in agency systems when such devices have no identifiable owner. [NIST 800-53 MP-7].

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
13 Apr 2018	Annual Review	2	DeAnn Seneff
29 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-10 to DCS 05-8250 for better tracking with Arizona Department	3	

	Homeland Security (AZDOHS) policy numbers.		
15 Mar 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 3/16/2024 Frank Sweeney Chief Information Officer AZDCS