



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
Physical Security Protection Policy	DCS 05-8260	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to protect DCS information systems and assets through limiting and controlling physical access and implementing controls to protect the environment in which DCS information systems and assets are housed. 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 Physical 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 agency IT PSPs within DCS;
2. ensure the Physical Security Protection 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 Physical Security Protection Policy for DCS;
 3. ensure all DCS personnel understand their responsibilities with respect to physical protection of agency information systems and assets.
- D. Supervisors of DCS employees and contractors shall:
1. ensure users are appropriately trained and educated on Physical 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 the physical protection of agency information systems and assets.

VI. POLICY

- A. Physical Access Authorizations [NIST 800-53 PE-2] [HIPAA 164.310 (a)(2)(iii)]
- DCS shall:
1. develop and maintain a list of individuals with authorized access to controlled areas or facilities where the DCS information system resides;
 2. issue authorization credentials based on job function;
 3. review and approve the access list and authorization credentials quarterly, and;
 4. remove individuals' access (including from the access list, keys, badges, and combination changes) when access is no longer required and immediately upon termination.
- B. Standard Physical Access Control [NIST 800-53 PE-3] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

DCS shall:

1. enforce physical access authorization at designated entry/exit points to the facility where the DCS information system resides;
2. verify individual access authorizations before granting access to the facility;
3. control ingress/egress to the facility using keys, locks, combinations, card readers, and/or guards;
4. Maintain physical access audit logs for DCS-defined entry and exit points;
5. Control access to areas within the facility designated as publicly accessible by implementing DCS-defined controls; and
6. provide cameras, monitoring by guards, or isolating selected DCS information system components (or any combination) to control access to areas within the facility officially designated as publicly accessible. Review collected data and correlate with other entries. Store at least 14 days unless otherwise directed by law.

C. Protected Physical Access Control

For all protected agency information systems and the server components of standard agency information systems for which additional physical protections apply, the BU shall [NIST 800-53 PE-3] [HIPAA 164.310(a)(1), (a)(2)(ii)]:

1. develop procedures to identify and authorize visitors;
2. develop procedures to easily distinguish between onsite personnel and visitors;
3. give visitors a physical token that expires and that identifies the visitors as onsite personnel and ensure the visitor surrenders the physical token before leaving the facility or at the date of expiration;
4. escort visitors and monitors visitor activity within controlled areas;
5. secure keys, combinations, and other physical access devices;
6. inventory keys and other physical access devices every quarter; keys and other physical access devices assigned to visitors are inventoried every

day, and;

7. change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or separated.

D. Monitoring Physical Access

DCS shall:

1. monitor physical access to the DCS information system to detect and respond to physical security incidents;
2. use video cameras and/or access control mechanisms (or both) to monitor physical access to sensitive areas;
3. review physical access logs weekly, and upon occurrence of potential indications of events;
4. coordinate results of reviews and investigations with the organizational incident response capability, and;
5. store physical access monitoring data for at least three (3) months.

E. Intrusion Alarms/Surveillance Equipment

DCS shall monitor real-time physical intrusion alarms and surveillance equipment [NIST 800-53 PE-6(1)].

F. Visitor Control Records

DCS shall:

1. maintain visitor access records to the controlled areas or facilities where the information system resides;
2. review visitor access records monthly and report anomalies in visitor access records to appropriate personnel [NIST 800-53 PE-8];
3. maintain a visitor log that includes the visitor's name, the firm represented, and the onsite personnel authorizing physical access;
4. retain the logs for a minimum of three (3) months;
5. limit Personally Identifiable Information Elements - DCS shall limit

personally identifiable information collected in visitor access records to DCS-defined elements identified in the system privacy risk assessment; [NIST 800-53 PE-8(3)]

G. Access Control

DCS shall implement the following physical access controls.

1. Transmission Medium – DCS shall control physical access to DCS information system distribution and transmission lines within DCS facilities using locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays [NIST 800-53 PE-4];
2. Workstations – DCS shall implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users [HIPAA 164.310(b), 164.310(c)].
3. Output Devices – DCS shall control physical access to DCS information system output devices to prevent unauthorized individuals from obtaining output [NIST 800-53 PE-5].
4. Network Jacks and Devices – DCS shall restrict physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
5. Power Equipment and Cabling – DCS shall protect power equipment and power cabling for the DCS information system from damage and destruction [NIST 800-53 PE-9].

H. Power

DCS shall implement the following physical controls for power.

1. Emergency Shutoff – DCS shall:
 - a. provide the capability of shutting off power to the DCS information system or individual system components in emergency situations;
 - b. place emergency shutoff switches or devices in data centers, server rooms, and computer rooms to facilitate safe and easy access for

personnel; and

- c. protect emergency power shut off capability from unauthorized activation.

2. Emergency Power – DCS shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss [NIST 800-53 PE-11].

I. Emergency Lighting

DCS shall employ and maintain automatic emergency lighting for the DCS information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility [NIST 800-53 PE-12].

J. Fire Protection

DCS shall employ and maintain fire suppression and detection devices/systems for the DCS information system that are supported by an independent energy source [NIST 800-53 PE-13].

1. Detection Devices – DCS shall employ fire detection devices/systems for the DCS information system that activate automatically and notify DCS and emergency responders in the event of a fire [NIST 800-53 PE-13(1)].
2. Suppression Devices – DCS shall employ fire suppression devices/systems for the DCS information system that provides automatic notification of any activation to DCS and emergency responders [NIST 800-53 PE-13(2)].
3. Inspections – DCS shall ensure the facility undergoes annual inspections by authorized and qualified inspectors and resolves identified deficiencies within 30 days [NIST 800-53 PE-13(3)].

K. Temperature and Humidity Controls

DCS shall maintain defined temperature and humidity levels within the facility where the DCS information system resides at data centers, server rooms, and computer rooms; and monitors temperature and humidity levels daily [NIST 800-53 PE-14].

L. Water Damage Protection

DCS shall protect DCS information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel [NIST 800-53 PE-15].

M. Delivery and Removal

DCS shall authorize, monitor, and control DCS information systems components entering and exiting the facility and maintain records of those items [NIST 800-53 PE-16].

N. Alternate Work Site

DCS shall:

1. determine and document the alternative work sites allowed for use by employee;
2. define and employ minimum security controls at alternate work sites;
3. assess, as feasible, the effectiveness of security controls at alternate work sites;
4. provide a means for employees to communicate with DCS information security personnel in case of security incidents or problems.

O. Development of Operational Procedures

DCS shall ensure that security policies and operational procedures for restricting physical access are documented, in use, and known to all affected parties.

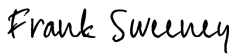
VII. DEFINITIONS

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
29 Dec 2021	Annual Review	2	DeAnn Seneff
29 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-11 to DCS 05-8260 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		<p>DocuSigned by:  <small>CDB46EB4E4A6442...</small> 3/13/2024</p> <p>Frank Sweeney Chief Information Officer AZDCS</p>