TITLE	POLICY NUMBER	
Access Control Policy	DCS 05-8320	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to define the correct use and management of logical access controls for the protection of DCS information systems and assets. 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

A. 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.

B. 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 Policies, Standards, and Procedures (PSPs);

2. ensure compliance with the DCS PSPs;

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 agency DCS IT PSPs;

2. 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 Access Control Policy for DCS;

3. ensure all DCS personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of DCS information systems and assets;

4. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems.

D. 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.

E. System Users of DCS information systems shall:

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

2. adhere to DCS PSPs regarding the correct use and management of logical access controls for the protection of agency information systems and assets.

VI. POLICY

A. Access Enforcement

1. DCS shall ensure DCS information system enforces approved authorizations for logical access to information and system resources in accordance with applicable control policies (e.g., identity-based policies, role-based policies) [NIST 800-53 AC-3] [HIPAA 164.308(a)(3)(ii)(A) - Addressable, 164.308 (a)(4)(ii)(B) & (C) - Addressable].

2. Assign Responsibility – DCS shall assign to an individual or team the Information Security management responsibility of monitoring and controlling all access to confidential data.

B. Development of Access Control Operational Procedures

DCS shall develop daily operational security procedures for restricting access to sensitive data are documented, in use, and known to all affected parties.

C. Information Flow Enforcement

DCS shall ensure DCS information system enforces approved authorizations for controlling the flow of information within the system and between connected systems based on DCS-defined information flow control policies, including Statewide Policy Framework 8350, Systems and Communications Protections. These policies prohibit direct public access between the internet and any system component in the protected DCS information system [NIST 800-53 AC-4].

1. Perimeter Firewalls for Wireless Networks – DCS shall install perimeter firewalls between any wireless network and the protected DCS information system, and configure these firewalls to deny, or control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment into the protected DCS information system.

2. Personal Firewalls – DCS shall require personal firewall software or equivalent functionality on any portable computing devices (including DCS and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access DCS network.

D. Least Privilege

DCS shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks. [NIST 800-53 AC-6].

1. Organizational Isolation – DCS shall implement policies and procedures that protect confidential information from unauthorized access by other (e.g., larger DCS to which DCS is a part of) organizations [HIPAA 164.308 (a)(4)(ii)(A)].

2. Shared Host Isolation – For agencies that provide a shared hosting service to other agencies, DCS shall ensure that DCS hosts are protected from other users and processes on the same host or environment. Specifically, that DCS shall ensure that:

   a. each entity only runs processes that have access to that entity's own environment, and

   b. each entity's access and privileges shall be restricted to its own environment.

3. Privileged Accounts – DCS shall restrict access rights to privileged user accounts to least privileges necessary to perform job responsibilities.

4. Job Classification – DCS shall restrict access rights based on individual personnel's job classification and function.

E. Authorize Access to Security Functions

DCS shall explicitly authorize access to the following security functions and security-relevant information [NIST 800-53 AC-6(1)]:

1. establishing security system accounts;

2. configuring security system access authorizations;

3. setting events to be audited;

4. setting intrusion detection parameters;

5. filtering rules for routers and firewalls;

6. cryptographic key management information;

7. configuration parameters for security services.

F. Non-Privileged Access for Non-Security Functions

DCS shall require that users of DCS information system accounts, or roles, with access to security functions (e.g., privileged users), use non-privileged accounts or roles, when accessing non-security functions [NIST 800-53 AC-6(2)].

G. Log Use of Privileged Function

DCS shall include execution of privileged functions in the events to be audited by DCS information system [NIST 800-53 AC-6(9)].

H. Prohibiting Non-Privileged Users from Executing Privileged Functions

DCS shall ensure DCS information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures [NIST 800-53 AC-6(10)].

I. Unsuccessful Logon Attempts

DCS shall ensure DCS information system enforces a DCS specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a DCS specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with the Statewide Access Control Standard 8320 [NIST 800-53 AC-7].

J. System Use Notification [NIST 800-53 AC-8]

DCS shall ensure that the DCS information system displays to users a DCS-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall state the following:

1. users are accessing an DCS information system owned by the DCS;

2. DCS information system usage may be monitored, recorded, and subject to audit;

3. unauthorized use of DCS information system is prohibited and subject to criminal and civil penalties;

4. use of DCS information system indicates consents to monitoring and recording;

5. retains the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access DCS information system;

6. for publicly accessible systems, the DCS information system shall also:

    a. display to users the system uses DCS information before granting further access;

    b. display to users references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;

    c. include in the notice given to public users of DCS information system, a description of the authorized uses of the system.

K. Session Lock

DCS shall ensure that the DCS information system prevents further access to the system by initiating a DCS-specified limit of time inactivity or upon receiving a request from a user; and retains the session lock for a DCS-specified limit of time or until the user re-establishes access using established identification and authentication procedures. If the user does not re-establish access within a DCS-specified limit of time, the session is dropped [NIST 800-53 AC-11] [HIPAA 164.312 (a)(2)(iii)].

1. Pattern-Hiding Display – DCS shall ensure that the system conceals, via the device lock, information previously visible on the display with a publicly viewable image. [NIST 800-53 AC-11(1)]:

2. Session Termination - DCS shall ensure that the system automatically terminates a user session after DCS-defined conditions or trigger events. [NIST 800-53 AC-12]

L. Permitted Access without Identification or Authentication

DCS shall identify user actions that can be performed on the DCS information system without identification or authentication consistent with DCS missions, and document and provide support rationale for user actions not requiring identification or authentication in the security plan for the DCS information system [NIST 800-53 AC-14].

M. Remote Access

DCS shall establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed, and authorize remote access to the DCS information system prior to allowing such connections [NIST 800-53 AC-17].

N. Automated Monitoring/Control

DCS shall ensure the DCS information system monitors and controls remote access methods (e.g., detection of cyber-attacks such as false logins and denial of service-attacks and compliance with remote access policies such as strength of encryption) [NIST 800-53 AC-17(1)].

1. Security Using Encryption – DCS shall ensure the DCS information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, consistent with

DCS policies [NIST 800-53 AC-17(2)].

2. Managed Access Control Points – DCS shall ensure the DCS information system routes all remote accesses through a limited number of managed network access control points [NIST 800-53 AC-17(3)].

3. Privileged Access Commands – DCS shall authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence, for BU-defined needs, and documents the rationale for such access in the security plan for the agency system. [NIST 800-53 AC-17(3)].

O. Wireless Access

1. DCS shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access, and authorize wireless access to DCS information system prior to allowing such connections that are consistent with DCS policies [NIST 800-53 AC-18].

2. Wireless Authentication and Encryption – DCS shall ensure the DCS information system protects wireless access to the DCS information system using authentication of users and devices and encryption [NIST 800-53 AC-18(1)].

3. Wireless Encryption Strength – DCS shall ensure that wireless networks transmitting confidential data use industry best practices to implement strong encryption for authentication and transmission.

4. Disable Wireless Networking - The BU shall disable, when not in use, wireless networking capabilities embedded within system components prior to issuance and deployment. [NIST 800-53 AC-18(3)].

P. Access Control for Mobile Devices

DCS shall establish configuration guidance, connection requirements, and implementation guidance for BU controlled mobile devices to include when such devices are outside of controlled areas; and authorizes connection of mobile devices to agency systems. [NIST 800-53 AC-19]

1. Full Device Encryption – DCS shall employ full-device or container-based encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to DCS information systems or to create, transmit, or process confidential information [NIST 800-53 AC-

19(5)] [HIPAA 164.308 (e)(2)(ii) - Addressable].

2. Purge or Wipe Mobile Device - DCS shall ensure that information on mobile devices are purged or wiped from mobile devices enabled for use with agency systems based on sanitization techniques using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250 after a BU-defined number of consecutive invalid logon attempts. [NIST 800-53 AC-7(2)]

Q. Use of External Information Systems (e.g., Back-up, Cloud Systems)

DCS shall establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store, or transmit DCS-controlled information using external information systems [NIST 800-53 AC-20].

DCS shall prohibit the use of DCS-defined types of external systems:

1. Limits on Authorized Use – DCS shall permit authorized individuals to use an external information system to access DCS information system to process, store, or transmit DCS controlled information only after DCS [NIST 800-53 AC-20(1)]:

   a. verifies the implementation of required security controls on the external system as specified in DCS information security policies and security plan;

   b. retains approved information system connection or processing agreements with the organizational entity hosting the external information system: The Arizona State Library, Archive and Public Records (ASLAPR) Information Technology (IT) Records GS-1064; Administrative and Management Records GS-1018 Rev.5; and DCS 02-24 Records Management.

2. Portable Storage Devices – DCS prohibits DCS-owned portable storage devices to be connected to external information systems (personally owned devices, vendor devices) of any kind. [NIST 800-53 AC-20(2)].

3. Restricted Use of Non-DCS Owned Systems - DCS shall restrict the use of DCS owned systems or system components to process, store, or transmit organizational information using DCS-defined restrictions [NIST 800-53

AC-20(3)].

R. Information Sharing

DCS shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access and use restrictions on the information for DCS-defined circumstances, and shall employ mechanisms or processes to assist users in making information sharing/collaboration decisions [NIST 800-53 AC-21].

1. Maintain List of Service Providers – DCS shall maintain a list of service providers, including a description of the service provided, that have access to confidential data;

2. Written Agreements – DCS shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of confidential data the service providers possess.

3. Due Diligence – DCS shall ensure there is an established process for engaging service providers, including proper due diligence prior to engagement.

4. Service Provider Monitoring Program – DCS shall maintain a program to monitor service provider's compliance with requirements for the protection of confidential data.

5. Service Provider Information – DCS shall maintain information about which information security requirements are managed by each service provider, and which are managed by DCS.

S. Publicly Accessible Content [NIST 800-53 AC-22]

DCS shall:

1. designate individuals authorized to post information onto a publicly accessible information system;

2. train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

3. review the proposed content of information prior to posting onto the publicly accessible DCS information system to ensure that nonpublic information is not included; and

4. review the content on the publicly accessible DCS information system for nonpublic information annually and removes such information, if discovered.

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	Matt Grant
31 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-15 to DCS 05-8320 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