Arizona Department of Child Safety

TITLE Account Management Policy	POLICY NUMBER DCS 05-8310	
RESPONSIBLE AREA DCS Information Technology	EFFECTIVE DATE March 07, 2024	REVISION 4

I. POLICY STATEMENT

The purpose of this policy is to establish the baseline controls for the administration of DCS information system accounts. 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 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 DCS PSPs;

3. 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 PSPs;

2. monitor employee activities to ensure compliance.

E. System Users of DCS information systems shall become familiar with and adhere to all DCS PSPs.

VI. POLICY

A. Account Management

DCS shall implement account management through the following activities.

1. Automated Account Management – DCS shall employ automated mechanisms to support the management of information system accounts [NIST 800-53 AC-2(1)].

2. Development of Account Management Operational Procedures – DCS shall ensure that security policies and operational procedures for restricting access to Confidential data are documented, in use, and known to all affected parties and cover all system components.

3. Identification of Account Types

DCS shall identify the types of DCS information system accounts to support organizational missions/business functions [NIST 800-53 AC-2a, AC-3] [HIPAA 164.312 (a)(2)(iii) – Addressable].

a. Establish Group and Role-based Accounts - DCS shall establish conditions for group and role membership [NIST 800-53 AC-2c, AC-3].

b. Account Specification – DCS shall specify authorized users of the DCS information system, group and role membership, and access authorizations (i.e., privileges) and other attributes for each account [NIST 800-53 AC-2d, AC-3].

c. Privileged Accounts – DCS shall restrict privileged accounts (e.g., Admin accounts) on the DCS information system to administrative roles [NIST 800-53 AC-6(5)].

d. Separation of Duties – DCS shall separate DCS-defined duties; document separation of duties of individuals; and define DCS information system access authorizations to support separation of duties [NIST 800-53 AC-5, AC-3].

B. Assignment of Account Manager

DCS shall assign account managers for DCS information system accounts [NIST 800-53 AC-2b].

C. Account Approval

1. DCS shall require documented approvals by authorized DCS staff for requests to create, modify, and enable DCS information system accounts [NIST 800-53 AC-2e-f].

2. Automated Audit Actions – DCS shall ensure the DCS information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required, DCS-defined personnel or roles [NIST 800-53 AC-2(4)].

D. Account Monitoring

1. DCS shall authorize and monitor the use of DCS information system accounts [NIST 800-53 AC-2g].

2. Vendor Account Monitoring – DCS shall enable accounts used by vendors for remote access only during the time period needed and monitor the vendor remote access accounts when in use.

E. Account Creation, Deletion, and Removal

DCS shall control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

1. Account Removal – DCS shall notify account managers when accounts are no longer required; users are separated or transferred; and individual information system usage or need-to-know changes [NIST 800-53 AC-2h].

2. Immediate Removal of Separated Users – DCS shall immediately revoke access for any separated users upon notification or a ServiceDesk ticket request.

3. Automatic Removal of Temporary Accounts – The DCS information system automatically removes or disables temporary and emergency accounts after a DCS-defined time [NIST 800-53 AC-2(2)].

4. Disable Inactive Accounts – DCS shall ensure the DCS information system automatically disables inactive accounts after DCS-defined time period [NIST 800-53 AC-2(3)].

F. Access Authorization

DCS shall authorize access to the DCS information system based on a valid access authorization; intended system usage; and other attributes as required by the organization or associated mission functions [NIST 800-53 AC-2f,i] [HIPAA 164.308 (4)(ii)(B) – Addressable].

1. Default "Deny All: Setting – DCS shall ensure the DCS information system access control system is set to "Deny all" unless specifically allowed.

2. Restrict Direct Database Access – DCS shall ensure the DCS information system authenticates all access to any database containing Confidential information and restricts direct access or queries to databases to database administrators.

G. Account Rights Review

DCS shall review accounts for compliance with account management requirements annually [NIST 800-53 AC-2j] [HIPAA 164.308 (4)(ii)(C) – Addressable].

H. Reissues of Account Credentials

DCS shall establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group [NIST 800-53 AC-2k]

I. Align with Termination Process

DCS shall align the account management processes with personnel termination and transfer processes. [NIST 800-53 AC-2i]

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 18	Initial Release	1	DeAnn Seneff
29 Dec 21	Annual Review	2	Matt Grant
30 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-14 to DCS 05-8310 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	Robert Navarro
XX 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