Arizona Department of Child Safety

TITLE System Security Audit Policy	POLICY NUMBER DCS 05-8330	
RESPONSIBLE AREA DCS Information Technology	EFFECTIVE DATE June 30, 2024	REVISION 4

I. POLICY STATEMENT

The purpose of this policy is to protect DCS information systems and data by ensuring DCS information systems have the appropriate controls and configurations to support audit log generation, protection, and review.

II. APPLICABILITY

This policy applies to all DCS information systems, processes, operations and personnel to include all 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 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 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:

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

VI. POLICY

A. Event Logging - DCS shall: [NIST 800-53 AU-2]

a. identify the types of events the agency system is capable of logging in support of the audit function;

b. coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection of criteria for events to be logged;

c. specify the event types for logging within the system as defined in the DCS-05-8330-S01 System Security Audit Standard along with the frequency of logging for each identified event type;

d. provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of security incidents;

e. ensure the events listed in the DCS System Security Audit Standard (DCS-05-8330-S01) are logged within DCS information system; and

f. review and update the selected audited events annually.

2. Content of Audit Records - DCS shall ensure that the DCS information system generates audit records containing information that establishes: [NIST 800-53 AU-3]

a. what type of event occurred;

b. when the event occurred;

c. where the event occurred;

d. the source of the event (i.e., name of the affected data, system component, or resource);

e. the outcome of the event; and

f. the identity of any individuals or subjects or objects/entities associated with the event.

3. Additional Audit Information - DCS shall ensure the state system information system generates audit records containing DCS-defined additional information. [NIST 800-53 AU-3(1)]

4. Audit Reviews and Updates - DCS shall review and update the selected audited events annually, or as required. [NIST 800-53 AU-2(3)]

5. Limit Personally Identifiable Information Elements - DCS shall limit personally identifiable information contained in audit records to the DCS-defined elements identified in the privacy risk assessment. [NIST 800-53 AU-3(3)

B. Audit Storage Capacity - DCS shall allocate audit record storage capacity to accommodate DCS-defined audit log storage requirements [NIST 800-53 AU-4].

C. Response to Audit Processing Failures - DCS shall ensure that the DCS information system alerts DCS-defined personnel or roles in the event of an audit logging process failure, and shuts down DCS information system, overwrites the oldest audit records, or stops generating audit records [NIST 800-53 AU-5].

1. Storage Capacity Warning - DCS shall ensure the agency system provides a warning to DCS-defined personnel when allocated audit log storage volume reaches a maximum capacity. [NIST 800-53 AU-5(1)]

D. Audit Review, Analysis, and Reporting - DCS shall: [NIST 800-53 AU-6] [HIPAA 164.308 (a)(1)(ii)(D)] [HIPAA 164.312 (b)]

a. review and analyze DCS information system audit records periodically for indications of inappropriate or unusual activity and the potential impact;

b. report findings to DCS-defined personnel or roles; and

c. adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

2. Process Integration - DCS shall integrate audit record review, analysis, and reporting processes using automated mechanisms. [NIST 800-53 AU-6(1)].

3. Correlate Audit Repositories: DCS shall analyze and correlate audit records across different repositories to gain DCS-wide situational awareness [NIST 800-53 AU6(3)].

E. Audit Reduction and Report Generation - DCS shall ensure the DCS information system provides and implements an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter original content or time ordering of audit records [NIST 800-53 AU-7].

1. Automatic Processing - DCS shall ensure the DCS information system provides and implements the capability to process, sort, and search audit records for events of interest based on the following audit fields within audit records [NIST 800-53 AU-7(1)]:

a. individual identities;

b. event types;

c. event locations;

d. event times and time frames;

e. event dates;

f. system resources involved, IP addresses involved;

g. information object accessed.

F. Time Stamps - DCS shall ensure the DCS information system uses internal system clocks to generate time stamps for audit records; and records time stamps for audit records that meet the BU-defined granularity of time measurement and that can use Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or have a fixed local time offset from UTC or GMT, or that include the local time offset as part of the time stamp. [NIST 800-53 AU-8]

1. Synchronization with Authoritative Time Source - DCS shall ensure the DCS information system compares the internal agency system clocks a BU-defined frequency with a DCS-defined time source and synchronizes the internal agency system clocks to the authoritative time source when the time difference is greater than a DCS-defined time period. [NIST 800-53 SC-45(1)]

2. Protection of Time Data - DCS shall ensure the DCS information system protects time-synchronization settings by restricting access to such settings to authorized personnel and logging, monitoring, and reviewing changes.

G. Protection of Audit Information - DCS shall ensure the DCS information system protects audit information and audit logging tools from unauthorized access, modification, and deletion; and alerts DCS-defined personnel upon detection of unauthorized access, modification, or deletion of audit information. [NIST 800-53 AU-9]

1. Access by Subset of Privileged Users - DCS shall authorize access and modification to management of audit logging functionality to only a DCS-defined subset of privileged users [NIST 800-53 AU-9(4)].

2. Audit Trail Backup - DCS shall promptly back up audit trail files to a centralized log server or media that is difficult to alter.

3. Audit Backup on Separate Physical Systems - DCS shall ensure the DCS information system backs up audit records onto a physically different system or system components than the system or component being audited.

4. File Integrity Monitoring of Audit Logs - DCS shall ensure the DCS information system uses file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts.

H. Audit Record Retention - DCS shall retain audit records for a DCS-defined time period consistent with the records retention policy with a DCS-defined time period available for immediate analysis to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. For agency systems with cardholder data these defined times are at least one year with a minimum of three months immediately available for analysis. [NIST 800-53 AU-11] [PCI DSS 10.7] DCS must comply with

Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 16.b.

I. Audit Generation - DCS shall ensure the agency system: [NIST 800-53 AU-12]

1. Provides audit record generation capability for the event types, defined in Section A (Event Loggins), at servers, firewalls, workstations, mobile devices, and other DCS-defined system components and services;

2. Anti-virus programs are generating audit logs;

3. Allows DCS-defined personnel or roles to select the event types that are to be logged by specific components of the agency system; and

4. Generates audit records for the event types, defined in Section A.c (Event Loggings), with the content defined in Section B (Content of Audit Records).

J. Cross Agency Auditing - DCS shall employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across DCS boundaries. Note: This requirement applies to outsourced data centers and cloud service providers. The provider must be held accountable to protect and share audit information with DCS through the contract. [NIST 800 53 AU-16]

K. Developing Operational Procedures - DCS shall ensure that security policies and operational procedures for monitoring all access to network resources and Confidential data are documented, in use, and known to all affected parties and cover all system components.

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
8 Jul 2020	Annual Review	2	Matt Grant
15 Aug 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-16 to DCS 05-8330 for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.	3	Frank Sweeney DCS CIO
30 June 2024	Annual review to mirror AzDoHS language	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS