



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
System Security Audit Policy	DCS 05-8330	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	August 15, 2023	3

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 Information Security Officer (ISO) 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. Audit Events

DCS shall:

1. determine that the DCS information system is capable of auditing the events listed in the DCS System Security Audit Standard (DCS 05-8330-S01);
2. coordinate the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
3. provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;
4. ensure the events listed in the DCS System Security Audit Standard (DCS-05-8330-S01) are logged within DCS information system;
5. for agencies that provide a shared hosting service to other agencies, ensure that logging and audit trails are unique to each agency's environment;
6. review and update the selected audited events annually, or as required [NIST 800-53 AU-2(3)].

B. Content of Audit Records

DCS shall ensure that the DCS information system generates audit records containing information [NIST 800-53 AU-3] that establishes:

1. what type of event occurred;
2. when the event occurred;
3. where the event occurred;
4. the source of the event (i.e., name of the affected data, system component, or resource);
5. the outcome of the event;
6. the identity of any individuals or subjects associated with the event.

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

C. Audit Storage Capacity

DCS shall allocate audit record storage capacity in accordance with DCS-defined audit record storage requirements [NIST 800-53 AU-4].

D. 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 processing failure, and shuts down DCS information system, overwrites the oldest audit records, or stops generating audit records [NIST 800-53 AU-5].

E. Audit Review, Analysis, and Reporting

DCS shall review and analyze DCS information system audit records periodically for indications of inappropriate or unusual activity, and report findings to DCS-defined personnel or roles.

1. Process Integration: DCS shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities [NIST 800-53 AU-6(1)].
2. Correlate Audit Repositories: DCS shall analyze and correlate audit

records across different repositories to gain DCS-wide situational awareness [NIST 800-53 AU6(3)].

F. Audit Reduction and Report Generation

DCS shall ensure the DCS information system provides 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 audit records [NIST 800-53 AU-7].

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

1. individual identities;
2. event types;
3. event locations;
4. event times and time frames;
5. event dates;
6. system resources involved, IP addresses involved;
7. information object accessed.

G. Time Stamps

DCS shall ensure the DCS information system uses internal system clocks to generate time stamps for audit records, generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), and provides a granularity of time to a DCS-defined unit of time [NIST 800-53 AU-8].

1. Synchronization with Authoritative Time Source - DCS shall ensure the DCS information system synchronizes internal DCS information system clocks a DCS-defined frequency with a DCS-defined time source when the time difference is greater than a DCS-defined time period [NIST 800-53 AU-8(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.

H. Protection of Audit Information

DCS shall ensure the DCS information system protects audit information and audit tools from unauthorized access, modification, and deletion. [NIST 800- 53 AU-9] [PCI DSS 10.5].

1. Access by Subset of Privileged Users - DCS shall authorize access and modification to management of audit 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.

I. Audit Record Retention

DCS shall retain audit records for a DCS-defined time period with a DCS-defined time period available for immediate analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements [NIST 800-53 AU-11].

J. Compliance with Arizona State Library, Archives and Public Records Rules

DCS must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting.

K. Audit Generation

DCS shall ensure the DCS information system [NIST 800-53 AU-12]:

1. provides audit record generation capability for the auditable events defined in section VI.A (Audit Events), at servers, firewalls, workstations, and other DCS-defined system components;
2. has anti-virus programs that generate audit logs;
3. allows DCS-defined personnel or roles to select which auditable events are to be audited by specific components of DCS information system;
4. generates audit records for the events, defined in Section VI.A (Audit Events), with the content defined in Section VI.B (Content of Audit Records).

L. 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.

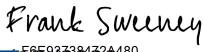
VII. DEFINITIONS

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	<p>DocuSigned by:  <small>F8592739817224480...</small> 8/17/2023</p> <p>Frank Sweeney CIO AZDCS</p>