ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
System Security Maintenance Policy	DCS 05-8220	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	May 20, 2025	5

I. POLICY STATEMENT

The purpose of this policy is to establish the baseline controls for management and maintenance of DCS information system controls.

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 DCS IT 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 IT 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 IT PSPs;

3. ensure all DCS personnel understand their responsibilities with respect to secure system management and maintenance.

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.

VI. POLICY

A. System Configuration Management

1. Configuration Management Plan – DCS shall develop, document, and implement a configuration management plan for DCS information systems that will:

   a. address the roles, responsibilities, and configuration management processes and procedures;

   b. establish a process for identifying configuration items throughout the software development lifecycle and for managing the configuration of the configuration items;

   c. define the configuration items for DCS information system and place the configuration items under configuration management;

   d. ensure configuration items are reviewed and approved by DCS-identified roles; and

   e. protect the configuration management plan from unauthorized disclosure and modification [National Institute of Standards and Technology (NIST) 800 53 CM-9].

2. Baseline Configuration – DCS shall develop, document, and maintain a

current baseline configuration of each DCS information system [NIST 800 53 CM-2].

a. Baseline Configuration Reviews and Updates – DCS shall review and update the baseline configurations for information systems at least annually, upon significant changes to system functions or architecture, and as an integral part of system installations and upgrades [NIST 800-53 CM-2].

i. Automated Support for Accuracy and Currency – DCS shall maintain currency, completeness, accuracy and availability of the baseline configuration of the systems using automated mechanisms, tools, or services. [NIST 800-53 CM-2(2)]

b. Baseline Configuration Retention – DCS shall retain at least one previous version of baseline configurations to support rollback. [NIST 800 53 CM-2 (3)]. However, DCS must comply with the Arizona State Library, Archive and Public Records (ASLAPR) rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Techn ology %20(IT).pdf Item 8.

c. Baseline Configuration for External High Risk Areas – DCS shall establish separate baseline configurations for computing resources (e.g., notebook computers) issued to individuals traveling to locations deemed to be a significant risk. The organization shall apply DCS-identified protective controls (e.g., examination for physical tampering, purge and reimage disk drives) to these devices when the individuals return from travel. [NIST 800-53 CM-2 (7)].

3. Configuration Change Control – DCS shall [NIST 800 53 CM-3]:

a. determine the types of changes to DCS information systems that are configuration-controlled;

b. review proposed configuration-controlled changes to DCS information systems and approves or disapproves such changes with explicit consideration for security impact analysis;

c. document configuration change decisions associated with DCS

information systems;

d.   implement approved configuration-controlled changes to the information systems;

e.   retain activities associated with configuration-controlled changes to DCS information system in compliance with the Arizona State Library, Archive and Public Records (ASLAPR) rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Techn ology% 20(IT).pdf Item 8;

f.   monitor and review activities associated with configuration-controlled changes to the information systems; and

g.   coordinate and provide oversight for configuration control activities through an established configuration control board that convenes at least monthly to review the activities associated with configuration-controlled changes to DCS information systems.

4.   Change Approval – DCS shall review and approve/disapprove proposed configuration-controlled changes to DCS information systems. Security and Privacy impact analysis shall be included as an element of the decision [NIST 800 53 CM-4].

a.   Test, Validate, and Document Changes – Approved changes shall only be implemented on an operational system after the change control board ensures that the change has been tested, validated, and documented [NIST 800 53 CM-3 (2)].

b.   Verification of Controls - After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regards to meeting the security and privacy requirements for the system. [NIST 800-53 CM-4(2)]

c.   Security and Privacy Representatives - Require that the change control board have representatives of security and privacy. [NIST 800-53 CM-3(4)]

5.   Change Restriction Enforcement – DCS shall ensure that adequate

physical and/or logical controls are in place to enforce restrictions associated with changes to DCS information systems. DCS shall permit only qualified and authorized individuals to access DCS information systems for the purpose of initiating changes, including upgrades and modifications [NIST 800 53 CM-5].

6. Configuration Settings – DCS shall [NIST 800 53 CM-6]:

    a. establish and document configuration settings for components employed within the agency system using Statewide, DCS information specific security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

    b. implement the configuration settings;

    c. identify, documents, and approve any deviations from established configuration settings for all information system components for which security checklists have been developed and approved; and

    d. monitor and control changes to the configuration settings in accordance with DCS Policies, Standards and Procedures (PSPs).

7. DCS Information System Component Inventory – DCS shall develop and document an inventory of DCS information system components (including authorized wireless access points and business justification for those access points) that accurately reflects the current DCS information system, is consistent with the defined boundaries of DCS information system, is at the level of granularity deemed necessary for tracking and reporting hardware and software, and includes hardware inventory specifications (e.g., manufacturer, device type, model, serial number, and physical location), software license information, software version numbers, component owners, and for networked components: machine names and network addresses. The inventory shall not duplicate an accounting of components assigned to any other system. [NIST 800 53 CM-8].

    a. Inventory Reviews and Updates – DCS shall review and update the information system component inventory annually and as an integral part of component installations, removals, and information system updates. [NIST 800 52 CM-8 (1)].

    b. Inventory Automated Detection – DCS shall detect the presence of unauthorized hardware, software, and firmware components within

the system using automated mechanisms quarterly, and take actions to disable network access, isolate the component, or notify the appropriate DCS personnel of the unauthorized component when unauthorized components are detected. [NIST 800 53 CM-8 (3)].

8. Confidential Information Location - DCS shall identify and document the location of Confidential data and specific components on which the information is processed and stored; identify and document the users who have access to the system and system components where the information is processed and stored; and document changes to the location where the information is processed and stored. [NIST 800-53 CM-12]

    a. Automated Tools to Support Confidential Information Location - DCS shall use automated tools to identify Confidential information on systems and system components to ensure controls are in place to protect DCS Confidential information and individual privacy. [NIST 800-53 CM-12(1)]

9. Software Usage Restrictions – DCS shall use software and associated documentation in accordance with contract agreements and copyright laws; track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work [NIST 800 53 CM-10].

B. Agency system Maintenance - In addition to the change management requirements of Section A, the following requirements apply to the maintenance of agency systems:

1. Controlled Maintenance – DCS shall [NIST 800 53 MA-2]:

    a. schedule, document, and review records of maintenance, repair and replacement on DCS information system components in accordance with manufacturer or vendor specifications and DCS requirements;

    b. approve and monitor all maintenance activities whether performed on site or remotely and whether the system or system components are serviced onsite or removed to another location;

    c.   explicitly approve the removal of DCS information system or system components from DCS facilities for offsite maintenance, repair or replacement;

    d.   sanitize equipment to remove Confidential information from associated media prior to removal from DCS facilities for off site maintenance, repair, or replacement;

    e.   ensure equipment removed from DCS facilities is properly sanitized prior to removal. (Refer to DCS 05-8250, Media Protection Policy, for appropriate sanitization requirements and methods); and

    f.   check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions. These checks are documented in DCS maintenance records and shall include date and time of maintenance, a description of the maintenance performed, names of individuals or groups performing the maintenance, the name of the escort (if applicable), and system components or equipment removed or replaced.

2.   Maintenance Tools – DCS shall approve, control, and monitor the use of system maintenance tools and shall review previously approved system maintenance tools annually. [NIST 800 53 MA-3].

    a.   Tool Inspection – Maintenance tools, and/or diagnostic and test programs carried into a DCS facility by maintenance personnel shall be inspected for improper or unauthorized modifications including malicious code prior to the media being used in DCS information systems [NIST 800 53 MA-3(1)(2)].

    b.   Prevent Unauthorized Removal - DCS shall prevent the removal of maintenance equipment containing Confidential information by verifying that there is no Confidential information contained on the equipment; sanitizing or destroying the equipment; retaining the equipment within the DCS facility; or obtaining an exemption from the DCS CISO explicitly authorizing removal of the equipment from the DCS facility. [NIST 800-53 MA-3(3)]

3.   Remote Maintenance – DCS shall: [NIST 800 53 MA-4]

a. approve and monitor remote maintenance and diagnostic activities;

b. allow the use of remote maintenance and ensure diagnostic tools are consistent with DCS policy and documented in the security plan for DCS information systems;

c. employ two-factor authentication for the establishment of remote maintenance and diagnostic sessions;

d. maintain records for all remote maintenance and diagnostic activities in compliance with the Arizona State Library, Archive and Public Records (ASLAPR) rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Techn ology% 20(IT).pdf Item 3; and

e. terminate network sessions and connections upon the completion of remote maintenance and diagnostic activities.

4. Maintenance Personnel – DCS shall [NIST 800 53 MA-5]:

a. establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. ensure non-escorted personnel performing maintenance on DCS information systems have required access authorizations;

c. designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

5. Timely Maintenance - DCS shall obtain maintenance support and/or spare parts for critical systems and system components within DCS-defined time periods of failure. [NIST 800-53 MA-6]

C. System and Information Integrity [HIPAA 164.132(c)(1)]

1. Flaw Remediation – DCS shall [NIST 800 53 SI-2]:

a. identify, report, and correct information system flaws;

b. test software and firmware updates related to flaw remediation are

tested for effectiveness and potential side effects prior to installation;

c. install security-relevant software and firmware updates and patches within 30 days of release from the vendor; and

d. incorporate flaw remediation into the organizational configuration management process.

2. Automated Flaw Remediation System – DCS shall employ an automated mechanism monthly to determine if system components have applicable security-relevant software and firmware updates installed. [NIST 800 53 SI-2(2)].

3. Malicious Code Protection – DCS shall [NIST 800 53 SI-3] [HIPAA 164.308(a)(5)(ii)(B) - Addressable]:

a. implement a centrally managed malicious code protection mechanisms at agency system entry and exit points and all systems commonly affected by malicious software particularly personal computers and servers to detect and eradicate malicious code; [NIST 800 53 SI-3, PL-9];

b. update malicious code protection mechanisms automatically whenever new releases are available in accordance with DCS's configuration management policy and procedures [NIST 800 53 SI-3]; and

c. Configure malicious code protection mechanisms to:

i. Perform weekly scan of the agency system and real-time scans of files from external sources at the endpoint, and network entry and exit points as the files are downloaded, opened, or executed;

ii. Block and quarantine malicious code and/or send an alert to a system administrator in response to malicious code detection;

iii. Generate audit logs; and

iv. all known types of malware

d. address the receipt of false positives during malicious code

detection and eradication and resulting potential impact on the availability of DCS information systems; and

e. Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period.

4. Information System Monitoring – DCS shall [NIST 800 53 SI-4a] [HIPAA 164.308(a)(1)(iii)(D)]:

a. monitor DCS information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections;

b. identify unauthorized use of DCS information systems through DCS-defined intrusion-monitoring tools;

c. Invoke internal monitoring capabilities or deploy monitoring devices strategically within the agency system, including at the perimeter and critical points inside the environment to collect essential security-relevant information and to track specific types of transactions of interest to DCS;

d. analyze detected events and anomalies;

e. adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the agency based on Confidential information;

f. receive alerts from:

    i. malicious code protection mechanisms;

    ii. intrusion detection or prevention systems;

    iii. boundary protection mechanisms such as firewalls, gateways, and routers;

g. obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations; and

h. provide state-defined system monitoring data to the state-defined

roles on a state-defined basis.

    i.   employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security and privacy implications. [NIST 800-53 SI-4(12)]

    j.   implement host-based monitoring mechanism on systems that receive, process, store, or transmit Confidential information. [NIST 800-53 SI-4(23)]

    k.   Updates – All intrusion detection systems and/or prevention engines, baselines, and signatures shall be kept up-to-date.

    l.   Automated Tools – DCS shall employ automated tools to support near real-time analysis of events [NIST 800-53 SI-4(2)].

    m.   Inbound and Outbound Communications Traffic – DCS shall determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic, monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. [NIST 800 53 SI-4(4)].

    n.   System Generated Alerts – DCS shall ensure the system alerts system administrators when the DCS-defined indicators of compromise or potential compromise occur. [NIST 800 53 SI-4(5)]

D.   Security Alerts, Advisories, and Directives - DCS shall implement a security alert, advisory and directive program to: [NIST 800 53 SI-5]:

    1.   receive information security alerts, advisories, and directives from DCS and additional services as determined necessary by DCS CISO on an on-going basis;

    2.   generate internal security alerts, advisories, and directives as deemed necessary;

    3.   disseminate security alerts, advisories, and directives to appropriate employees and contractors, other organizations, business partners, supply chain partners, external service providers, and other supporting organizations as deemed necessary; and

    4.   implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

E.   Integrity Verification Tools - DCS shall employ integrity verification tools to detect unauthorized changes to critical software, system files, configuration files, or content files. Upon detection of such changes DCS shall perform DCS-defined actions. [NIST 800 53 SI-7] [HIPAA 164.312(c)(1)].

    1.   Integrity Checks – DCS shall ensure DCS information systems will perform integrity checks at least weekly and at start up, the identification of a new threat to which DCS information systems are susceptible, and the installation of new hardware, software, or firmware [NIST 800-53 SI-7(1)].

    2.   Automated Notifications of Integrity Violations - DCS shall employ automated tools that provide notification to DCS-defined personnel or roles upon discovering discrepancies during integrity verification. [NIST 800-53 SI-7(2)]

    3.   Incident Response Integration – DCS shall incorporate the detection of unauthorized changes to critical system files into DCS incident response capability [NIST 800-53 SI-7(7)].

F.   Spam Protection

DCS shall employ spam protection mechanisms at DCS information system entry and exit points to detect and take action on unsolicited messages and updates spam protection mechanisms automatically updated when new releases are available. [NIST 800-53 SI8, 8(2)].

    1.   Central Management – Spam protection mechanisms are centrally managed. [NIST 800-53 PL-9].

    2.   Automated Updates - Spam protection mechanisms automatically update daily. [NIST 800-53 SI-8(2)]

    3.   Continuous Learning Capability - Spam protection mechanisms incorporate a learning capability to more effectively identify legitimate communications traffic. [NIST 800-53 SI-8(3)].

G.   Information Input Validation - DCS shall ensure DCS information systems check the validity of information system inputs from untrusted sources, such as user input [NIST 800-53 SI-10].

H.   Error Handling - DCS shall ensure that the DCS information system generates error messages that provide information necessary for corrective actions without

revealing information that could be exploited by adversaries and reveals error messages only to system administrator roles [NIST 800-53 SI-11].

I. Information Management and Retention - DCS shall handle and retain information within the agency system and information output from the system in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [NIST 800-53 SI-12] [ARS 44-7041] [Arizona State Library Retention Schedules for Information Technology (IT) Records]

1. DCS shall limit personally identifiable information being processed in the information life cycle to DCS-defined elements of personally identifiable information. [NIST 800-53 S-12(1)]

2. DCS shall use DCS-defined techniques to minimize the use of personally identifiable information for research, testing, or training. [NIST 800-53 SI-12(2)]

3. DCS shall use the techniques consistent with those defined in the DCS-05-8250 Media Protection Policy and to dispose of, destroy, or erase information following the retention period in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [NIST 800-53 SI-12(3)] Arizona State Library Retention Schedules for Information Technology (IT) Records]

J. Memory Protection – DCS shall ensure the system implements controls to protect the system memory from unauthorized code execution. [NIST 800-53 SI-16].

K. Establish Operational Procedures – DCS shall ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
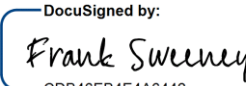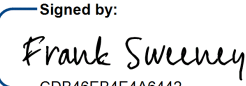
VII. DEFINITIONS

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
06 Dec 2017	Initial Release	1	DeAnn Seneff
02 Jul 2018	Annual Review	2	DeAnn Seneff
09 Jun 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-07 to DCS 05-8220 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	Frank Sweeney DCS CIO
30 Jun 2024	Annual review to mirror AzDoHS language	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS
20 May 2025	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	5	Signed by: Frank Sweeney CDB46EB4E4A6442... 6/2/2025 Frank Sweeney Chief Information Officer AZDCS