



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
System Security Maintenance Policy	DCS 05-8220	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	June 9, 2023	3

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 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 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. 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 (1)].
- 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: [Information Technology \(IT\) Records GS-1064](#) Records Series Number 20781; [Administrative and Management Records GS-1018 Rev.5](#); [Department of Child Safety](#); and [DCS 02-24 Records Management](#).
 - c. Baseline Configuration for High Risk Areas – DCS shall establish separate baseline configurations for identified high risk areas [NIST 800-53 CM-2 (7)].
3. Change Control Board – 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: [Information Technology \(IT\) Records GS-1064](#) Records Series Number 20781; [Administrative and Management Records GS-1018 Rev.5](#); [Department of Child Safety](#); and [DCS 02-24 Records Management](#);
 - f. 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 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-4 (3)].
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 CM5].
6. Configuration Settings – DCS shall [NIST 800 53 CM-6]:
 - a. establish and document configuration settings for information technology products employed within DCS information systems using 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;
 - d. monitor and control changes to the configuration settings in accordance with DCS PSPs.
7. DCS Information System Component Inventory – DCS shall develop and document an inventory of DCS information system components 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 [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 employ automated mechanisms to detect, quarterly, the presence of unauthorized hardware, software, and firmware components within DCS information system and take actions to disable network access, isolate the component, or notify the appropriate DCS personnel of the unauthorized component [NIST 800 53 CM-8 (3)].
8. 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. DCS Information System Maintenance

In addition to the System Configuration Management requirements of Section A, the following requirements apply to the maintenance of DCS information systems:

1. Controlled Maintenance – DCS shall [NIST 800 53 MA-2]:
 - a. schedule, perform, document, and review records of maintenance and repairs on DCS information system components in accordance with manufacturer or vendor specifications and DCS requirements;
 - b. approve and monitor all maintenance activities whether performed onsite or remotely and whether the equipment is 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 or repair;
 - d. 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);
 - e. check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. These checks are documented in DCS maintenance records.
2. Maintenance Tools – DCS shall approve, control, and monitor DCS information system maintenance tools [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 MA3(1)(2)].
3. Remote Maintenance

DCS shall document in the security plan for DCS information system the policies and procedures for the installation and use of remote maintenance and diagnostics are documented connections [NIST 800 53 MA-4(2)].
DCS shall also [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:

[Information Technology \(IT\) Records GS-1064](#) Records Series Number 20781; [Administrative and Management Records GS-1018 Rev.5](#); [Department of Child Safety](#); and [DCS 02-24 Records Management](#);

- 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.
- C. System and Information Integrity [HIPAA 164.132(c)(1)]
- 1. Flaw Remediation (software/firmware patching) – 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;
 - d. incorporate flaw remediation into the organizational configuration management process.
 - 2. Automated Flaw Remediation System – DCS shall employ an automated mechanism monthly to determine the state of the information system components with regard to flaw remediation [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. employ centrally managed malicious code protection mechanisms at DCS information systems 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(2)];
 - 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(1)];
 - c. address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of DCS information systems;
 - d. configure malicious code protection mechanisms to:
 - i. perform periodic scan of DCS information system weekly 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;
 - iv. ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by the DCS CIO or designee 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. deploy monitoring devices strategically within DCS information systems, including at the perimeter and critical points inside the environment to collect essential security relevant data and to track specific types of transactions of interest to DCS;
 - d. protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
 - e. heighten the level of monitoring activity within the intrusion monitoring systems whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or DCS based on Confidential information;
 - f. receive alerts from malicious code protection mechanisms;
 - g. receive alerts from intrusion detection or prevention systems;
 - h. receive alerts from boundary protection mechanisms such as firewalls, gateways, and routers;
 - i. obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations.
- 5. Updates – All intrusion detection systems and/or prevention engines, baselines, and signatures shall be kept up-to-date.
 - 6. Automated Tools – DCS shall employ automated tools to support near real-time analysis of events [NIST 800-53 SI-4(2)].
 - 7. Inbound and Outbound Traffic – DCS shall monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions [NIST 800 53 SI-4(4)].
 - 8. System Generated Alerts – DCS shall implement the information monitoring system to alert system administrators when the following indications 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 ISO 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;
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 system files, configuration files, or content files [NIST 800 53 SI-7] [IRS Pub 1075] [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. 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 SI-8(1)].

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. Output Handling and Retention

DCS shall handle and retain information within DCS information 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].

J. 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.

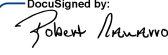
VII. DEFINITIONS

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	 6/12/2023 Robert Navarro Deputy Director Arizona Department of Child Safety