



*Arizona Department of Child Safety*

TITLE	POLICY NUMBER	
System Security Acquisition and Development Policy	DCS 05-8130	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	August 15, 2023	3

## I. POLICY STATEMENT

The purpose of this policy is to establish adequate security controls for the acquisition and deployment of DCS information systems.

## 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, Sept 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 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;
4. appoint a DCS Data Chief that shall be responsible for following the guidelines set forth in [P4400 – Data Governance Organization Policy](#).

B. The DCS Chief Information Officer (CIO) shall:

1. work with the DCS Director to ensure the correct and thorough completion of agency IT PSPs within DCS;
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. DCS Procurement Official shall:
1. provide advice and support with the procurement of goods and services in regards to request for information, request for proposal, evaluation of response, and contract awards;
  2. ensure compliance with Arizona procurement statutes and DCS PSPs throughout the procurement process.
- E. DCS Purchasers shall:
1. abide by all DCS PSPs throughout the procurement process.
- F. Supervisors of DCS employees and contractors shall:
1. ensure users are appropriately trained on this and all DCS PSPs;
  2. monitor employee activities to ensure compliance.
- G. System Users of DCS information systems shall:
1. become familiar with and adhere to all DCS PSPs;

## **VI. POLICY**

- A. Allocation of Resources - DCS shall [NIST 800 53 SA-02]:
1. determine information security requirements for DCS information systems or information system services in mission/business process planning;
  2. determine, document and allocate the resources required to protect DCS information systems or information system services as part of its capital

planning and investment control process; and

3. establish a discrete line item for information security in organizational programming and budgeting documentation.

B. Technology Life Cycle

1. DCS shall [NIST 800 53 SA-03]:
  - a. manage DCS information system using a DCS-defined technology life cycle that is based on industry standards or best practices and incorporates information security considerations;
  - b. define and document information security roles and responsibilities throughout the technology life cycle;
  - c. identify individuals having information security roles and responsibilities; and
  - d. integrate the organizational information security risk management process into technology life cycle activities.
2. Software Development Process - DCS shall require developers of DCS information systems or system components to implement the following software development processes:
  - a. Remove non-production application accounts, user IDs, and passwords before applications become active or are released to customers; and
  - b. Review custom code prior to release to production or customers in order to identify any potential coding vulnerability. Review shall be performed by someone other than the code author and by someone knowledgeable of code review techniques and secure coding practices; based on secure coding guidelines; and reviewed and approved by management.
3. Change Control Procedures - DCS shall require developers of DCS information systems, or system components, to follow change control processes and procedures for all changes to system components. The

process must:

- a. ensure separate development/test and production environments;
  - b. ensure production data is not used for testing or development;
  - c. ensure removal of test data and accounts before production systems become active;
  - d. include documentation of the impact;
  - e. include documented change approval by authorized parties;
  - f. include functionality testing to verify that the change does not adversely impact the security of the system;
  - g. include back-out procedure; and
  - h. upon completion of a significant change, ensure that all relevant security requirements are implemented on all new or changed systems and networks, and documentation updated as applicable.
4. Secure Coding Guidelines - DCS shall require developers of DCS information systems, or system components, to develop applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes, to include the following:
- a. injection flaws, particularly SQL injection (also consider OS Command Injection, LDAP and XPath injection flaws, as well as other injection flaws);
  - b. buffer overflow;
  - c. insecure cryptographic storage;
  - d. insecure communications;
  - e. improper error handling;
  - f. all "High" vulnerabilities identified in the vulnerability

identification process; and

- g. for web applications and web application interfaces:
  - i. Cross-site scripting (XSS);
  - ii. Improper Access Control (such as direct object references, failure to restrict URL access, and directory traversal);
  - iii. Cross-site request forgery (CSRF);
  - iv. Broken authentication and session management.

### C. Acquisition Process

1. DCS shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs [NIST 800 53 SA-04]:
  - a. security functional requirements;
  - b. security strength requirements;
  - c. security assurance requirements;
  - d. security-related documentation requirements;
  - e. requirements for protecting security-related documentation;
  - f. description of the information system development environment and environment in which the system is intended to operate; and
  - g. acceptance criteria.
2. Functional Properties of Security Controls - DCS shall require the developer of DCS information system, system component, or information system service to provide a description of the functional properties of the

security controls to be employed [NIST 800 53 SA-04(1)].

3. Design/Implementation Information for Security Controls - DCS shall require the developer of DCS information system, system component, or DCS information system service to provide design and implementation information for the security controls to be employed that includes: [NIST 800 53 SA04(2)]:
  - a. security-relevant external system interfaces; and
  - b. high-level design.
4. Services in Use - DCS shall require the developer of DCS information system component, or DCS information system service, to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use [NIST 800 53 SA-04(9)].

D. State Information System Documentation - DCS shall [NIST 800 53 SA-05]:

1. obtain administrator documentation for DCS information system, system component, or DCS information system service that describes:
  - a. secure configuration, installation, and operation of the system, component, or service;
  - b. effective use and maintenance of security functions/mechanisms; and
  - c. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
2. obtain user documentation for DCS information system, system component, or DCS information system service that describes:
  - a. user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
  - b. methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner;

- c. user responsibilities in maintaining the security of the system, component, or service;
    - d. protecting documentation as required, in accordance with the risk management strategy; and
    - e. ensuring documentation is available to DCS-defined personnel or roles.
- E. Security Engineering Principles - DCS shall apply information system security engineering principles in the specification, design, development, implementation, and modification of DCS information systems [NIST 800 53 SA-08].
- F. External Information System Services
  - 1. DCS shall [NIST 800 53 SA-09]:
    - a. require that providers of external DCS information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidance;
    - b. define and document government oversight and user roles and responsibilities with regard to external information system services; and
    - c. employ Service Level Agreements (SLAs) to monitor security control compliance by external service providers on an ongoing basis [HIPAA 164.308(b)(1); 164.314(a)(2)(i)].
  - 2. Identification of Services - DCS shall require providers of external DCS information system services to identify the functions, ports, protocols, and other services required for the use of such services [NIST 800 53 SA-09(2)].
- G. Develop Configuration Management - DCS shall require the developer of DCS information system, system component, or DCS information system service to [NIST 800 53 SA-10]:



1. perform configuration management during system, component, or service (development, implementation, and operation);
2. document, manage, and control the integrity of changes to configuration items under configuration management;
3. implement only DCS-approved changes to DCS information systems;
4. document approved changes to the system, component, or service and the potential security impacts of such changes, and
5. track security flaws and flaw resolution within the system, component, or service.

#### H. Develop Security Testing and Evaluation

1. DCS shall require the developer of DCS information system, system component, or DCS information system service to [NIST 800 53 SA-11]:
  - a. create and implement a security assessment plan that provides for security testing and evaluation, at the depth of security-related functional properties, including:
    - i. security-related externally visible interfaces;
    - ii. high-level design; and
    - iii. at the rigor of demonstrating.
  - b. perform integration and regression testing for components and services and unit, integration, and system testing for systems;
  - c. produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
  - d. implement a verifiable flaw remediation process; and
  - e. correct flaws identified during security testing/evaluation.
2. Public Web Application Protections - DCS shall require the provider of

DCS information system service for public-facing web applications to address new threats and vulnerabilities on an ongoing basis and to ensure that these applications are protected against known attacks by either of the following methods:

- a. reviewing public-facing web applications using manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or
  - b. installing a web-application firewall in front of public-facing web applications.
3. Threat and Vulnerability Analyses - DCS shall require the developer of DCS information system, system component, or DCS information system service to perform threat and vulnerabilities analyses and subsequent testing/evaluation of the as-built system, component, or service [NIST 800 53 SA-11(2)].
  4. Independent Verification of Assessment Plans / Evidence - DCS shall require an independent agent to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation [NIST 800 53 SA-11(3)].
  5. Penetration Testing / Analysis - DCS shall perform penetration testing to include black box testing by skilled security professionals simulating adversary actions and with automated code reviews [NIST 800 53 SA-11(5)].
  6. Establish Operational Procedures – DCS shall ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

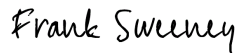
## **VII. DEFINITIONS**

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
<b>06 Dec 2017</b>	Initial Release	1	DeAnn Seneff
<b>02 Jul 2018</b>	Annual Update	2	DeAnn Seneff
<b>15 Aug 2023</b>	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-05 to DCS 05-8130 System Security Acquisition and Development Policy for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.	3	<p>DocuSigned by:    <small>F6E93738472A480...</small>  8/17/2023</p> <p>Frank Sweeney  CIO  AZDCS</p>