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	June 30, 2024	4

VI. POLICY STATEMENT

The purpose of this policy is to establish adequate security controls for the acquisition and deployment of DCS information systems. This Policy will be reviewed annually.

VII. 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.

VIII. 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

IX. 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**

X. ROLES AND RESPONSIBILITIES

C. 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.

D. 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.

E. 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.

F. 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.

G. DCS Purchasers shall:

1. abide by all DCS PSPs throughout the procurement process.

H. 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.

I. System Users of DCS information systems shall:

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

XI. POLICY

C. Allocation of Resources - DCS shall [NIST 800 53 SA-2]:

1. determine the high-level information security and privacy 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.

D. Technology Life Cycle - DCS shall [NIST 800 53 SA-03]:

i. 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;

ii. define and document information security roles and responsibilities throughout the technology life cycle;

iii. identify individuals having information security roles and responsibilities; and

iv. integrate the organizational information security risk management process into technology life cycle activities.

1. Software Development Process - DCS shall require developers of DCS information systems or system components to implement the following software development processes:

i. Remove non-production application accounts, user IDs, and passwords before applications become active or are released to customers; and

ii. 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.

2. 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:

    i. ensure separate development/test and production environments;

    ii. ensure separation of duties between development/test and product environments

    iii. ensure production data is not used for testing or development; and

    iv. ensure removal of test data and accounts before production systems become active;

    v. include documentation of the impact;

    vi. include documented change approval by authorized parties;

    vii. include functionality testing to verify that the change does not adversely impact the security of the system;

    viii. include back-out procedure; and

    ix. 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.

3. 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:

    i. injection flaws, particularly SQL injection (also consider OS Command Injection, LDAP and XPath injection flaws, as well as other injection flaws);

ii. buffer overflow;

iii. insecure cryptographic storage;

iv. insecure communications;

v. improper error handling;

vi. all “High” vulnerabilities identified in the vulnerability identification process; and

vii. for web applications and web application interfaces:

(a) Cross-site scripting (XSS);

(b) Improper Access Control (such as direct object references, failure to restrict URL access, and directory traversal);

(c) Cross-site request forgery (CSRF);

(d) Broken authentication and session management.

E. Acquisition Process - 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]:

i. security and privacy functional requirements;

ii. security strength requirements;

iii. security and privacy assurance requirements;

iv. Controls needed to satisfy the security and privacy requirements;

v. Security and privacy documentation requirements;

vi. requirements for protecting security and privacy documentation;

vii. description of the information system development environment and environment in which the system is intended to operate;

viii. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

ix. acceptance criteria.

1. 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)].

2. 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)]:

   i. security-relevant external system interfaces; and

   ii. high-level design.

3. Services in Use - DCS shall require the developer of DCS information system component, or DCS information system service to identify the functions, ports, protocols, and services intended for organizational use. [NIST 800 53 SA-4(9)]

4. Use of Approved PIV Products - The BU shall employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within BU systems. [NIST 800-53 SA-4(10)]

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

a. obtain or develop administrator documentation for DCS information system, system component, or DCS information system service that describes:

i. secure configuration, installation, and operation of the system, component, or service;

ii. effective use and maintenance of security functions/mechanisms; and

iii. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

b. obtain or develop user documentation for DCS information system, system component, or DCS information system service that describes:

i. user-accessible security and privacy functions/mechanisms and how to effectively use those security functions and mechanisms;

ii. methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy;

iii. user responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

iv. ensure documentation is available to DCS-defined personnel or roles.

G. Security Engineering Principles - DCS shall apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of DCS information systems [NIST 800 53 SA-08].

1. Personally Identifiable Information Minimization - DCS shall

implement the privacy principle of minimization using DCS-defined processes. [NIST 800-53 SA-8(33)]

H. External Information System Services - DCS shall [NIST 800 53 SA-09]:

i. require that providers of external DCS information system services comply with organizational information security and privacy requirements and employ security controls in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance;

ii. define and document organizational oversight and user roles and responsibilities with regard to external information system services; and

iii. employ Service Level Agreements (SLAs) to monitor control compliance by external service providers on an ongoing basis [HIPAA 164.308(b)(1); 164.314(a)(2)(i)].

a. 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)].

b. Processing, Storage, and Service Location - The BU shall restrict the location of systems that receive, process, store, or transmit Confidential information to areas within the United States territories, embassies, or military installations. [NIST 800-53 SA-9(5)]

I. 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 system, component, or service;

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.

J. Develop Security Testing and Evaluation - DCS shall require the developer of DCS information system, system component, or DCS information system service at all post-design stages of the system development life cycle, to [NIST 800 53 SA-11]:

i. Develop and implement a plan for ongoing security and privacy control assessments; Perform integration and regression testing for components and services and unit, integration, and system testing for systems;

ii. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

iii. Implement a verifiable flaw remediation process; and

iv. Correct flaws identified during security testing and evaluation.

b. 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:

i. reviewing public-facing web applications using manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or

ii. installing a web-application firewall in front of public-facing web applications.

2. Threat and Vulnerability Analyses - DCS shall require the developer of DCS information system, system component, or DCS information system service to perform threat modeling and vulnerabilities analyses during development and subsequent testing and evaluation of system, component, or service that: [NIST 800 53 SA-11(2)].

   i. Uses the DCS-defined contextual information concerning impact, environment of operations, known or assumed threats, and acceptable risks;

   ii. Employs DSC-identified tools and methods;

   iii. Conducts the modeling and analyses at the DCS-defined level of rigor; and

   iv. Produces evidence that meets the DCS-defined acceptance criteria.

3. Independent Verification of Assessment Plans / Evidence - DCS shall: [NIST 800 53 SA-11(3)]

   i. require an independent agent to verify the correct implementation of the developer security and privacy assessment plan and the evidence produced during security testing and evaluation.

   ii. Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.

4. Penetration Testing / Analysis - DCS shall require the developer of the agency system, system component, or agency system service to 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)]

K. 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.

XII. DEFINITIONS

Refer to the Policy, Standards and Procedures Glossary located on the Arizona Strategic Enterprise Technology (ASET) website.

XIII. ATTACHMENTS

None.

XIV. REVISION HISTORY

Date	Change	Revision	Signature
06 Dec 2017	Initial Release	1	DeAnn Seneff
02 Jul 2018	Annual Update	2	DeAnn Seneff
15 Aug 2023	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	Frank Sweeney DCS CIO
30 Jun 2024	Annual review to mirror AZDoHS Policy	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS