ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
Information Security Program Policy	DCS 05-8120	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	May 20, 2025	5

I. POLICY STATEMENT

The purpose of this policy is to establish the information security program and responsibilities within the Department of Child Safety (DCS). This policy will be reviewed annually.

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 or Designee, 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 Information Technology Policies, Standards, and Procedures (PSPs) within DCS;

2. ensure DCS compliance with the Information Security Program Policy;

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 within the BU;

2. ensure all DCS managed systems have submitted the following documents for approval by the State CIO or designated alternate by July 1 of each year:

a. a complete list of information systems with a system classification

DCS 05-8120 Information Security Program Policy originally published December 6, 2017

assignment and system owner for each DCS information system;

b. a system security plan and system security assessment plan for each protected DCS information system;

c. a Plan of Actions and Milestones (POAM) for each protected DCS information system.

3. ensure information security risks to DCS information systems, are adequately addressed according to the DCS information system risk assessment documentation;

4. be the system owner for all DCS information systems or delegate a system owner for DCS information system.

C. The DCS Chief Information Security Officer (CISO) shall:

1. advise the DCS CIO on the completeness and adequacy of DCS provided documentation and reports, and recommend a course of action where security risks are not adequately addressed;

2. ensure all system owners understand their responsibilities for the security planning, management, and authorization of DCS information systems;

3. ensure the correct execution of the system security assessment plans.

D. The DCS Privacy Officer shall:

1. advise the State CISO and the State CPO on the completeness and adequacy of the DCS activities and documentation provided to ensure compliance with privacy laws, regulations, statutes and Statewide IT Privacy PSPs throughout all agency BUs;

2. assist the agency to ensure the privacy of sensitive personal information within DCS's possession;

3. assist with the development, implementation, reviews, and approves DCS privacy Policies, Standards, and Procedures (PSPs) related to the Privacy Act to assure that personal information is handled in compliance and requested exceptions from the statewide privacy PSPs;

4. identify and convey to the DCS CIO the privacy risk to agency information systems and data based on current implementation of privacy

controls and mitigation options to improve privacy;

5. serve as the DCS advisor in consultation with legal relating to public disclosure of information and any identified privacy issues.

E. DCS System Owner shall:

1. be responsible for the overall procurement, development, integration, modification, or operation and maintenance of the DCS information system;

2. advise the DCS CISO as to the DCS information system categorization;

3. ensure creation of required system security plans, system security assessment plans, and Plan of Actions and Milestones (POAM);

4. ensure the implementation of information security controls as described in system security plans and POAM.

F. 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.

G. System Users of DCS information systems shall:

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

VI. POLICY

A. System Security Planning

DCS shall implement the following controls in the planning of system security:

1. System Security Plan – DCS shall develop, distribute, review annually, and update a DCS information system security plan. The plan shall [NIST 800-53 PL-2]:

a. be consistent with DCS enterprise architecture (EA);

b. explicitly define the authorization boundary for the system

including authorized connected devices (e.g., smart phones, authorized virtual office computer equipment, and defined external interfaces);

c. describe the operational context of the DCS information system in terms of missions and business processes;

d. identify the individuals that fulfill system roles and responsibilities;

e. identify the information types processed, stored, and transmitted by the system;

f. provide the security categorization of the information system, including supporting rationale;

g. describe any specific threats to the system that are of concern to the Agency;

h. provide the results of a privacy risk assessment for systems processing personally identifiable information;

i. describe the operational environment for the system and any dependencies on or connections to other systems or system components;

j. provide an overview of the security and privacy requirements for the system;

k. identify any relevant control baselines or overlays, if applicable;

l. describe the controls in place or planned for meeting the security and privacy requirements including rationale for any tailoring decisions;

m. include risk determinations for security and privacy architecture and design decisions;

n. include security- and privacy-related activities affecting the system that require planning and coordination with the CIO, CISO, and system owners of affected agency information systems; and

o. be reviewed and approved by DCS CIO or designee prior to plan implementation.

2.   Security and Privacy Architecture

DCS shall: [NIST 800-53 PL-8]

    a.   develop an information security architecture for the DCS information system that describes:

        i.   the requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

        ii.   how the information security architecture is integrated into and supports the enterprise architecture;

        iii.   any information security dependencies on, and assumptions regarding, external systems and services.

    b.   annually review and update the information security architecture to reflect updates in the enterprise architecture; and

    c.   reflect planned information security architecture changes in the security privacy plans and organizational procedures, and procurements/acquisitions.

B.   System Security Policies

1.   DCS shall develop security, privacy, and supply chain management risk policies and procedures to address the associated risk with the operation and use of agency information systems and the authorized processing of personally identifiable information. These policies and procedures shall include the following:

    a.   DCS-05-8110 Data Classification Policy and Procedures

    b.   DCS-05-8111 Policy Administration Policy

    c.   DCS-05-8120 Information Security Program Policy and Procedures, including security, privacy, and supply chain risk management [NIST 800-53 CA-1] [NIST 800-53 PL-1] [NIST 800-53 PM-1] [NIST 800-53 RA-1][SR-1]

    d.   DCS-05-8130 System Security Acquisition Policy and Procedures [NIST 800-53 SA-1]

  e. DCS-05-8210 Security Awareness Training Policy and Procedures [NIST 800-53 AT-1]

  f. DCS-05-8220 System Security Maintenance Policy and Procedures [NIST 800-53 CM-1] NIST 800-53 MA-1] [NIST 800-53 SI-1]

  g. DCS-05-8230 Contingency Planning Policy and Procedures [NIST 800-53 CP-1]

  h. DCS-05-8240 Incident Response Planning Policy and Procedures [NIST 800-53 IR-1]

  i. DCS-05-8250 Media Protection Policy and Procedures [NIST 800-53 MP-1]

  j. DCS-05-8260 Physical Security Protection Policy and Procedures [NIST 800-53 PE-1]

  k. DCS-05-8270 Personnel Security Policy and Procedures [NIST 800-53 PS-1]

  l. DCS-05-8280 Acceptable Use Policy, including social media, networking restrictions, restrictions on posting on public websites, and use of organizational identifiers [NIST 800 53 AC-1] [NIST SP 800 53 PL-4a, PL-4(1)]

  m. DCS-05-8310 Account Management Policy and Procedures

  n. DCS-05-8320 Access Controls Policy and Procedures [NIST 800-53 AC-1] [HIPAA 164.310 (a)(2)(ii)]

  o. DCS-05-8330 System Security Audit Policy and Procedures [NIST 800-53 AU-1]

  p. DCS-05-8340 Identification and Authentication Policy and Procedures [NIST 800-53 IA-1]

  q. DCS-05-8350 System and Communication Protections Policy and Procedures [NIST 800-53 SC-1]

  r. DCS-05-8410 System Privacy Policy and Procedures

  s. DCS-05-8410-1 System Privacy Notice

2.   Policy Development, Maintenance and Distribution

DCS shall [HIPAA 164.316 (a), (b)(1), (b)(2)]:

a.   designate an agency official to develop, document and disseminate, to appropriate personnel and roles, the policies and procedures for each agency information system;

b.   maintain the organizational security policies, standards, and procedures;

c.   these policies shall be consistent with applicable laws, directives, regulations, policies, standards, and guidelines.

d.   retain these documents for six years from the date of its creation or the date it last was in effect, whichever is later. However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to https://apps.azlibrary.gov/records/general_rs/GS%201018%20Rev.5.pdf;

e.   make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

f.   review documentation at least annually, and update as needed, in response to environmental or operational changes affecting the security of the confidential information.

C.   Risk Management

To appropriately manage security risk to DCS information systems, the following activities shall be performed for each DCS information system [HIPAA 164.308 (a)(1)(i), (a)(1)(ii)(B)]:

1.   Impact Assessment – A potential impact assessment shall be performed for each DCS information system to determine the system categorization. An impact assessment considers the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the DCS information system and/or its data. Impact assessments result in the determination of impact based on the following definitions:

a. Limited Adverse Impact – The loss of confidentiality, integrity, or availability could be expected to have limited adverse effect on organizational operations, organizational assets or individuals. For example, it may:

   i. cause a degradation in mission capability, to an extent and duration, that the organization is able to perform its primary function, but the effectiveness of the function is noticeably reduced;

   ii. result in minor damage to organizational assets;

   iii. result in a minor financial loss; or

   iv. result in minor harm to individuals.

b. Serious Adverse Impact – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals. For example, it may:

   i. cause significant degradation in mission capability, to an extent and duration, that the organization is able to perform its primary function, but the effectiveness of the function is significantly reduced;

   ii. result in significant damage to organizational assets;

   iii. result in a significant financial loss; or

   iv. result in significant harm to individuals that do not involve loss of life or serious life-threatening injuries.

   (Note: Impact assessment on DCS information systems storing, processing, or transmitting Confidential Data may result in a serious adverse impact).

2. System Categorization

   DCS shall categorize DCS information systems and the information it processes, stores, and transmits, document the security categorization results (including supporting rationale) in the security plan for the DCS information system, and ensure that the security categorization decision is

reviewed by DCS CISO and approved by DCS CIO or Designee. All agency information systems are categorized according to the potential impact to the State or citizens resulting from the disclosure, modification, destruction, or non-availability of system functions or data. [NIST 800-53 RA-2].

3.   System Categorization Levels

The following system categorization levels shall be applied to all DCS information systems:

a.   Standard – Loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact on DCS operations, organizational assets, or individuals, including citizens;

b.   Protected – Loss of confidentiality, integrity, or availability could be expected to have serious, severe, or catastrophic adverse impact on organizational, assets, or individuals, including citizens.

4.   Risk Assessment

DCS shall [NIST 800-53 RA-3] [HIPAA 164.308 (a)(1)(ii)(A)]:

a.   conduct an assessment of security and privacy risk, including identification of threats to and vulnerabilities in the system, the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the agency information system, the information it processes, stores, or transmits, and any related information;

    i.   determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

    ii.   integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

    iii.   perform and document the risk assessment annually or whenever there are significant changes to the information system or environment of operations (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

   iv. review risk assessment results annually;

   v. disseminate risk assessment results to the DCS CIO, DCS CISO, agency information system owner, and other DCS-defined personnel or roles; and

 b. Conduct an assessment of supply chain risks associated with DCS systems, system components, and system services. The supply chain risk assessment shall be updated annually, when there are significant changes to the supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. [NIST 800-53 RA-3(1)].

5. Vendor Risk Management

DCS shall protect against vendor (e.g., Cloud Service Providers, contractors, supply chain) threats to the information system, system component, or information service by employing a vendor risk management program as part of a comprehensive, defense in-breadth information security strategy [NIST 800-53 SA-12][SR-1].

6. Third Party Risk Assessment

DCS shall conduct an assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, modification, or destruction of third parties authorized by DCS to process, store, or transmit confidential data [HIPAA 164.308 (a)(ii)(A)].

7. Vulnerability Scanning

DCS shall establish a process to identify security vulnerabilities implementing the following [NIST 800-53 RA-5]:

 a. use reputable outside sources for security vulnerability information;

 b. assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities;

 c. monitor and scan for vulnerabilities in the DCS information system and hosted applications quarterly and when new vulnerabilities potentially affecting the system/applications are identified and reported from internal and external interfaces;

  d. employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

    i. enumerating platforms, software flaws, and improper configurations;

    ii. formatting checklists and test procedures; and

    iii. measuring vulnerability impact.

  e. analyze vulnerability scan reports and results from vulnerability monitoring within 30 days in accordance with an organizational assessment of risk;

  f. remediate legitimate vulnerabilities within 30 days in accordance with an organization assessment of risk;

  g. share information obtained from the vulnerability monitoring process and control assessments with DCS-defined personnel or roles to help eliminate similar vulnerabilities in other DCS information systems (i.e. systemic weaknesses or deficiencies.);

  h. establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components; [NIST 800-53 RA-5(11)];

  i. establish a process to identify and assign risk ranking to newly discovered security vulnerabilities;

  j. address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved according to vulnerability ranking.

    i. Update tool capability – DCS shall employ vulnerability scanning tools that include the capability to readily update the DCS information system vulnerabilities to be scanned [NIST 800-53 RA-5].

    ii. Update prior to new scans – DCS shall update the DCS information system vulnerabilities scanned prior to new scans [NIST 800-53 RA-5(2)].

    iii. Provide Privileged Access – DCS information system

implements privileged access authorization to DCS-defined components containing highly confidential data (e.g., databases) [NIST 800-53 RA-5(5)].

iv.   Quality Scanning Vendors – DCS shall employ an impartial and qualified scanning vendor to conduct quarterly external vulnerability scanning. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the DCS information systems under assessment and is qualified in the use and interpretation of vulnerability scanning software and techniques.

D.   Information Security Program Management

DCS shall implement the following controls in the management of the information security program:

1.   Senior Information Security Officer (ISO) – DCS shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a DCS-wide information security program [NIST 800-53 PM-2] [EO 2008-10].

2.   Information Security Resources – DCS shall include the resources needed to implement the information security program and document all exceptions to this requirement. This includes employing a business case to record the resources required, and ensuring that information security resources are available for expenditure as planned.

3.   Plan of Action and Milestones Process

DCS shall [NIST 800-53 PM-4]:

a.   implement a process for ensuring that plans of action and milestones for the security program, privacy, and supply chain risk management programs and associated DCS information systems are:

i.   developed and maintained;

ii.   reported in accordance with DCS reporting requirements;

iii.   documented with the remedial information security,

privacy, and supply chain management actions to adequately respond to risk to organizational operations, assets, individuals, other organizations, and the State.

b. review plans of action and milestones for consistency with the organizational risk management strategy and DCS-wide priorities for risk response actions.

4. Systems Inventory

DCS shall develop and annually update an inventory of its information systems, including a classification of all system components (e.g., Standard or Protected) [NIST 800-53 PM-5].

5. Measures of Performance

DCS shall develop, monitor, and report on the results of information security and privacy measures of performance [NIST 800-53 PM-6].

6. Enterprise Architecture

DCS shall develop and maintain an enterprise architecture with consideration for information security, privacy, and resulting risk to organizational operations, organizational assets, individuals, other organizations, and DCS [NIST 800-53 PM-7].

7. Critical Infrastructure Plan

If applicable, DCS shall address information security, and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan [NIST 800-53 PM-8].

8. Risk Management Strategy

DCS shall:

a. develop a comprehensive strategy to manage security risk to organizational operations and assets, individuals, other organizations, and the agency associated with the operation and use of DCS information systems; privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. implement this strategy consistently across the organization and

    c.   Review and update the risk management strategy annually or as required to address organizational changes. [NIST 800-53 PM-9].

9.   Supply Chain Risk Management Strategy - DCS shall [NIST 800-53 SR-2]:

    a.   develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems, system components, or system services;

    b.   review and update the supply chain risk management plan annually or as required to address threat, organizational, or environmental changes;

    c.   protect the supply chain risk management plan from unauthorized disclosure and modification;

    d.   establish a supply chain risk management team to lead and support the supply chain risk management activities [NIST 800-53 SR-2(1)];

    e.   implement supply chain risk management controls and processes, including: [NIST 800-53 SR-3]

        i.   establishing a process(es) to identify and address weaknesses or deficiencies in the key supply chain elements and processes in coordination with supply chain personnel;

        ii.   employing adequate controls to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related event; and

        iii.   documenting the selected and implemented supply chain processes and controls in the supply chain risk management plan;

    f.   employ appropriate acquisition strategies, contract tool, and procurement methods to protect against, identify, and mitigate supply chain risks [NIST 800-53 SR-5];

g. assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [NIST 800-53 SR-6];

h. establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessments or audits [NIST 800-53 SR-8];

i. inspect the appropriate systems or system components randomly but at sufficient frequency to adequately detect tampering [NIST 800-53 SR-10];

j. develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and report counterfeit system components to the source of the counterfeit component and the State CISO. DCS shall [NIST 800-53 SR-11]:

   i. train appropriate personnel to detect counterfeit system components (including hardware, software, and firmware) [NIST 800-53 SR-11(1)];

   ii. maintain configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service [NIST 800-53 SR-11(2)].

k. dispose of system components using the approved techniques and methods that ensure the sanitization of sensitive data [NIST 800-53 SR-12].

10. Risk Response - DCS shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with DCS-defined risk tolerance [NIST 800-53 RA-7].

11. Privacy Impact Assessments - DCS shall conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that processes personally identifiable information and before initiating a new collection of personally identifiable information that will be processed using information technology and includes personally identifiable information permitting the

physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than DCSs or state employees [NIST 800-53 RA-8].

12.   Criticality Analysis - DCS shall identify critical system components and functions by performing a criticality analysis for DCS systems, system components, and system services when the system is being designed, modified, or upgraded [NIST 800-53 RA-9].

13.   Security Authorization Process

DCS shall [NIST 800-53 PM-10]:

a.   manage the security state of organizational information systems and the environments in which those systems operate through security authorization processes;

b.   designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c.   fully integrate the security authorization processes into a DCS-wide risk management program.

14.   Mission/Business Process Definition

DCS shall [NIST 800-53 PM-11]:

a.   define mission/business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and DCS; and

b.   determine information protection needs and personally identifiable information processing needs arising from the defined mission/business processes; and

c.   revise the process as necessary, until achievable protection needs are obtained.

15.   Insider Threat Program

DCS shall implement an insider threat program that includes a cross-discipline insider threat incident handling team [NIST 800-53 PM-12].

16.   Information Security Workforce

DCS shall establish an information security and privacy workforce development and improvement program [NIST 800-53 PM-13].

17.   Testing, Training, and Monitoring

DCS shall [NIST 800-53 PM-14]:

a.   implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained; and continue to be executed in a timely manner; and

b.   review testing, training, and monitoring plans for consistency with the organizational risk management strategy and DCS-wide priorities for risk response actions.

18.   Contacts with Security Groups and Associations – DCS shall establish and institutionalize contact with selected groups and associations within the security community to [NIST 800-53 PM-15]:

a.   facilitate ongoing security education and training for DCS personnel;

b.   maintain currency with recommended security practices, techniques, and technologies; and

c.   share current security-related information including threats, vulnerabilities, and incidents.

E.   Control Assessments and Authorizations

DCS shall implement the following controls in the assessment and authorization of DCS information systems:

1.   Control Assessments – DCS shall: [NIST 800-53 CA-2]

a. develop a control (e.g., security and privacy controls) assessment plan that describes the scope of the assessment including security controls under assessment, assessment procedures to be used to determine security control effectiveness, and assessment environment, assessment team, and assessment roles and responsibilities;

b. assess the controls in the information system and its environment of operation quarterly to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. produce a control assessment report that documents the results of the assessment; and

provide the results of the security control assessment to DCS CIO or Designee, DCS CISO, DCS Privacy Officer and State CISO.

2. Independent Assessors – DCS shall employ impartial assessors or assessment teams to conduct control assessments. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the DCS information systems under assessment [NIST 800-53 CA-2(1)].

3. Third Party Security Assessment – DCS shall conduct a security assessment with third parties authorized by DCS that process, store, or transmit confidential data [HIPAA 164.308 (a)(8)].

4. Wireless AP Testing – DCS shall test for the presence of wireless access points and detect unauthorized wireless access points on an quarterly basis.

5. System Interconnections – DCS shall [NIST 800-53 CA-3]:

a. authorize connections from the DCS information system to other information systems through the use of Interconnection Security Agreements; information exchange agreements; memorandum of understanding or agreement; service level agreement; user agreements; or nondisclosure agreements;

b. document, for each interconnection, the interface characteristics, security and privacy requirements, controls and responsibilities for

each system, and the impact level of the information communicated; and

c.   review and update agreements annually.

    i.   Restrictions on External System Connections - DCS shall employ a "deny-all, permit-by-exception" policy for allowing protected DCS information systems to connect to external information systems at managed interfaces [NIST 800-53 SC-7(5)].

    ii.   Third Party Authorization – DCS shall permit a third party, authorized by DCS to process, store, or transmit confidential data to create, receive, maintain, or transmit confidential information on DCS's behalf only if the covered entity obtains satisfactory assurances that the third party will appropriately safeguard the information. DCS documents the satisfactory assurance through a written contract or other arrangement with the third party [HIPAA 164.308 (b)(1) and (b)(2)].

6.   Plan of Action and Milestones

DCS shall: [NIST 800-53 CA-5]

a.   develop a plan of action and milestones for the DCS information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b.   update existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

7.   Security Authorization

DCS shall [NIST 800-53 CA-6]:

a.   assign a senior-level executive or manager as the authorizing official for the information system and accepting common controls inherited by Statewide or other organizational systems;

b.   ensure the authorizing official authorizes the DCS information system for processing and accepts the inherited common controls before commencing operations; and

c.   update the security authorization every three years;

8.   Continuous Monitoring

DCS shall develop a system-level continuous monitoring strategy and implements a DCS-level or continuous monitoring program that includes [NIST 800-53 CA-7] [HIPAA 164.308 (a)(1)(ii)(D)]:

a.   establishment of system-level metrics to be monitored;

b.   establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;

c.   ongoing security control assessments in accordance with DCS continuous monitoring strategy;

d.   ongoing security status monitoring of DCS-defined system-level metrics in accordance with DCS continuous monitoring strategy;

e.   correlation and analysis of security-related information generated by assessments and monitoring;

f.   response actions to address results of the analysis of security-related information; and

g.   reporting the security status of DCS and the information system to DCS CISO quarterly;

h.   Employing independent assessors or assessment teams to monitor the controls in the system on an ongoing basis; [NIST 800-53 CA-7(1)].

i.   Ensuring risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness, compliance, and change monitoring. [NIST 800-53 CM-7(4)].

9.   Penetration Testing

DCS shall conduct penetration testing annually and after significant infrastructure or application upgrade or modification on protected DCS information systems from internal and external interfaces. These penetration tests must include network-layer penetration tests, segmentation control tests, and application-layer penetration tests [NIST 800-53 CA-8].

a. Independent Penetration Agent or Team – DCS shall employ an impartial penetration agent or penetration team to perform penetration testing. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of DCS information systems under assessment [NIST 800-53 CA-8].

b. Segmentation Testing – DCS shall ensure that penetration testing includes verification of segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all Protected systems and components systems from non-protected systems and components.

c. Address Penetration Testing Issues – DCS shall ensure that exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

10. Internal System Connections

DCS shall authorize internal connections of other DCS information systems or classes of components (e.g., digital printers, laptop computers, mobile devices, facsimile machines, sensors, and servers) to the DCS information system and, for each internal connection, shall document the interface characteristics, security and privacy requirements, and the nature of the information communicated. DCS shall terminate internal system connections after the need for such connections is no longer required and shall review these connections annually [NIST 800-53 CA-9].

F. Establish Operational Procedures

DCS shall ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties, and any remediation actions taken are documented.
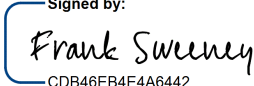
VII.   DEFINITIONS

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
31 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-04 to DCS 05-8120 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	Robert Navarro
01 July 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/18/2024 Frank Sweeney Chief Information Officer AZDCS

DCS 05-8120 Information Security Program Policy originally published December 6, 2017

| 20 May 2025 | Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions | 5 | Signed by:
 Frank Sweeney
 CDB46EB4E4A6442...
 5/20/2025

 Frank Sweeney

 Chief Information Officer

 AZDCS |