Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
System and Communication Protection	DCS 05-8350	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	July 22, 2025	5

I. POLICY STATEMENT

The purpose of this policy is to establish the baseline controls for the protection of Department of Child Safety (DCS) information systems and their communications. This Policy will be reviewed annually.

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, September 2020.

IV. EXCEPTIONS

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

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 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 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 PSPs;

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems.

D. 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.

E. System Users of DCS information systems shall:

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

VI. POLICY

A. Network and Architecture Controls - DCS shall ensure the DCS information system implements the following network and network architectural controls.

1. Application Partitioning - DCS shall ensure the DCS information system separates user functionality, including user interface services, either physically or logically from DCS information system management functionality (e.g., privileged access) [NIST 800 53 SC-2].

2. Boundary Protection - DCS shall ensure the DCS information system [NIST 800 53 SC-7]:

a. monitors and controls communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. implements sub-networks for publicly accessible system components that are logically or physically separated from internal organizational networks; and

c. connects to external networks or systems only through managed interfaces consisting of boundary protections devices arranged in accordance with organizational security and privacy architecture.

3. Implement DMZ (demilitarized zone) - DCS shall ensure the DCS information system prohibits direct public access between the Internet and

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

any system component in the protected DCS information system. The DMZ:

a. limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports;

b. limits inbound Internet traffic to IP addresses within the DMZ;

c. implements anti-spoofing measures to detect and block forged source IP addresses from entering the network;

d. does not allow unauthorized outbound traffic from the Protected DCS information system to the Internet;

e. permits only "established" connections into the network;

f. places system components that store Confidential data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks; and

g. does not disclose private IP addresses and routing information to unauthorized parties (Note: methods to obscure IP addressing may include: Network Address Translations (NAT), placing servers behind proxy servers, removal route advertisements for private networks that employ registered addressing, or internal use of RFC 1918 address space instead of registered addresses).

4. Firewall Configuration Standards - DCS shall establish and implement firewall and router configuration standards that include the following:

a. a formal process for approving and testing all network connections and changes to the firewall and router configurations;

b. current network diagrams that identifies all connections between DCS information system and other networks, including any wireless networks;

c. current diagram that shows all Confidential data flows across systems and networks;

d. requirements for a firewall at each Internet connection and between any DMZ and the Internal network zone;

e. description of groups, roles, and responsibilities for management

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

of network components;

f. documentation and business justification for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure;

g. requirement to review firewall and router rule sets at least every six (6) months;

5. Firewall Configuration - DCS shall build firewall and router configurations that restrict access points between non-protected systems (standard DCS information systems or untrusted networks) and any system components in the protected DCS information system. The configurations:

a. restrict inbound and outbound traffic to that which is necessary for the Protected DCS information system;

b. secure and synchronize router configuration files; and

c. implement perimeter firewalls between all wireless networks and the Protected DCS information system, and these firewalls are configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Protected DCS information system.

6. Limit Access Points - DCS shall limit the number of external network connections to the DCS information system [NIST 800 53 SC-7(3)].

7. Deny by Default/Allow by Exception - DCS shall ensure the DCS information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception) [NIST 800 53 SC-7(5)].

8. Network Disconnect - DCS shall ensure DCS information system terminates the network connections associated with a communications session at the end of the session or after 15 minutes of inactivity [NIST 800 53 SC-10].

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

B. Server Controls - DCS shall ensure the DCS information system implements the following controls for servers and components of the DCS information system:

1. Information in Shared Resources: DCS shall ensure DCS information system prevents unauthorized and unintended information transfer using shared system resources [NIST 800 53 SC-4].

2. Prevent Split Tunneling for Remote Devices: DCS shall ensure the DCS information system prevents split tunneling for remote devices connecting to agency systems unless the split tunnel is securely provisioned using a VPN that locks connectivity to exclusive, managed, and names environments, or to a specific set of pre-approved addresses, without user control. [NIST 800 53 SC-7(7)]

3. Route Traffic to Authenticated Proxy Servers - DCS shall ensure the agency system routes DCS-defined internal communications traffic to DCS-defined external networks through authenticated proxy servers at managed interfaces. [NIST 800 53 SC-7(8)]

4. Personally Identifiable Information - DCS shall ensure that agency systems that process personally identifiable information: [NIST 800 53 SC-7(24)]

    a. Applies DCS-defined processing rules to data elements of personally identifiable information;

    b. Monitors for permitted processing at the external interfaces to the agency system and at key internal boundaries within the agency system;

    c. Documents each processing exception; and

    d. Reviews and removes exceptions that are no longer supported.

5. Single Primary Function (Database): DCS shall ensure DCS information system components (e.g., servers) implementing a database implement only one primary function (the database) on this server.

6. Least Functionality - DCS shall ensure the agency system and system components (e.g., server) are configured to provide only necessary capabilities for the function of the system; and prohibit or restrict the use of unnecessary or nonsecure services, software, protocols, system ports, daemons, or services. [NIST 800 53 CM-7]

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

a. Otherwise Protected - For all other DCS information systems unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be disabled or removed.

b. Implement additional security features for any required services, protocols, or daemons that are considered to be nonsecure.

c. Periodic Review - DCS shall annually review the system to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and disable or remove these elements within the system deemed unnecessary or nonsecure. [NIST 800 53 CM-7(1)]

d. Prevent Program Execution - DCS shall ensure that the agency system is configured to prevent program execution in accordance with DCS-defined policies; rules of behavior; access agreements regarding software program usage and restrictions, and rules authorizing the terms and conditions of software program usage. [NIST 800 53 CM-7(2)]

e. Authorized Software - Allow By Exception - DCS shall identify DCS-defined software programs authorized to execute on the agency system; employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the agency system, and review and update the list of authorized software programs annually. [NIST 800 53 CM-7(5)]

7. Secure Configuration - DSC shall configure DCS information system component (e.g., server) security parameters to prevent misuse.

C. Secure Services - DCS shall ensure the DCS information system implements the following controls for services provided:

1. Denial of Service Protection - DCS shall ensure the DCS information system protects against or limits the effects of the types of denial of service attacks, defined in DCS-05-8350-S01 System and Communication Protection Standard, by employing boundary protection devices with packet filtering capabilities and, if required by DCS, employing increased capacity and bandwidth combined with service redundancy [NIST 800 53 SC-5].

2. Cryptographic Services - DCS shall ensure the DCS information system

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

implements the following cryptographic services:

a. Cryptographic Protection – DCS information system shall determine the DCS-defined cryptographic uses and implement state defined types of cryptography for each specified cryptographic use and in accordance with applicable federal and state laws, Executive orders, directives, policies, regulations, and standards. [NIST 800 53 SC-13] [HIPAA 164.312(a)(2)(iv), (e)(2)(i)]

b. Cryptographic Key Establishment and Management - DCS shall establish and manage cryptographic keys when cryptography is employed within the agency system in accordance with statewide requirements for key generation, distribution, storage, access, and destruction. [NIST 800 53 SC-12].

3. Key Protection - DCS shall protect all keys used to secure Confidential data against disclosure and misuse by:

   a. restricting access to cryptographic keys to the fewest number of custodians necessary; and

   b. storing secret and private keys used to encrypt/decrypt Confidential data in one (or more) of the following forms at all times:

      i. encrypted with a key-encrypting key that is at least as strong as the data-encrypting key;

      ii. within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device);

      iii. as at least two full-length key components or key shares, in accordance with an industry accepted method;

   c. storing cryptographic keys securely in the fewest possible locations.

4. Key Management Process - DCS shall fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of Confidential data including the following:

   a. generation of strong cryptographic keys;

   b. secure cryptographic key distribution;

   c. secure cryptographic key storage;

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

d. cryptographic key changes for keys that have reached the end of their crypto-period, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines;

e. retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened, or keys are suspected of being compromised;

f. if manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control;

g. prevention of unauthorized substitution of cryptographic keys;

h. requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

5. Public Key Infrastructure Certificates - DCS shall ensure the agency system issues public key certificates under a state defined certificate policy or obtains them from an approved service provider; and includes only approved trust anchors in trust stores or certificate stores management by the state or agency [NIST 800 53 SC-17]

6. External Telecommunications Services – DCS shall [NIST 800 53 SC-7(4)]:

a. implement a managed interface for each external telecommunication service;

b. establish a traffic flow policy for each managed interface;

c. protect the confidentiality and integrity of the information being transmitted across each interface;

d. document each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

e. review exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

7. Transmission Confidentiality and Integrity - DCS shall ensure the DCS information system protects the confidentiality and, if required, integrity of transmitted information [NIST 800 53 SC-8] [HIPAA 164.312(c)(1), (c)(2), (e)(1)].

   a. Cryptographic or Alternate Physical Protection - DCS shall ensure DCS information system prevents unauthorized disclosure of information and detects changes to information during transmission. [NIST 800 53 SC-8(1)] [HIPAA 164.312(c)(1), (c)(2), (e)(1)].

8. Mobile Codes - DCS shall [NIST 800 53 SC-18]:

   a. define acceptable and unacceptable mobile code and mobile code technologies (e.g., Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript); and

   b. authorize, monitor, and control the use of mobile code within DCS information system.

9. Collaborative Computing Devices - DCS shall ensure the DCS information system prohibits remote activation of collaborative computing devices and applications with the following exceptions: cameras and microphones in support of remote conferences and training; and provides an explicit indication of use to users physically present at the devices [NIST 800 53 SC-15].

10. Session Authenticity - DCS shall ensure the DCS information system protects the authenticity of communication sessions. Note: This control addresses communications protections at the session, versus packet level and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking and the insertion of false information into sessions [NIST 800 53 SC-23].

11. Secure Name/Address Resolution Service – DCS shall ensure the DCS

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

information system implements the following with respect to secure name/ address resolution service:

a. Secure Name/Address Resolution Service (Authoritative Service) – DCS shall ensure the DCS information system provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace [NIST 800 53 SC-20].

b. Secure Name/Address Resolution Service (Recursive or Caching Resolver) - DCS shall ensure the DCS information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources [NIST 800 53 SC-21].

c. Architecture and Provisioning for Name/Address Resolution Service - DCS shall ensure the DCS information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation [NIST 800 53 SC-22].

12. Protection of Information at Rest - DCS shall ensure the DCS information system protects the confidentiality and integrity of data at rest [NIST 800 53 SC-28].

a. Cryptographic Protection - DCS shall ensure the agency system implements cryptographic mechanisms to prevent unauthorized disclosure and modification on DCS-defined data at rest on DCS-defined system components. [NIST 800 53 SC-28]

13. Process Isolation - DCS shall ensure the agency system maintains a separate execution domain for each executing system process. [NIST 800 53 SC-39]

D. Establish Operational Procedures - DCS shall ensure that security policies and operational procedures for managing firewalls (including managing vendor defaults and other security parameters and protecting Confidential data) are documented, in use, and known to all affected parties.

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

E. Change Vendor Defaults - DCS shall ensure that vendor-supplied defaults are always changed and default accounts are removed or disabled before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.).

1. Change Wireless Vendor Defaults - for wireless environments connected to DCS information system or transmitting Confidential data change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

F. Configuration Standards - DCS shall ensure that configuration standards for all system components are developed. DCS shall assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to:

1. Center for Internet Security (CIS);

2. International Organization for Standardization (ISO);

3. National Institute of Standards and Technology (NIST).

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
02 Jul	Initial Release	1	DeAnn Seneff

Docusign Envelope ID: 71F6BBF4-C28A-4EA9-AC54-80A700017B50

2018			
8 Jul 2020	Annual Review	2	Matt Grant
22 Aug 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-18 to DCS 05-8350 System and Communication Protection Policy for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.	3	Frank Sweeney AZDCS CIO
30 Jun 2024	Annual changes to match AZDoHS Policy updates	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS
22 Jul 2025	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	5	Signed by: Frank Sweeney CDB46EB4E4A6442... 7/22/2025 Frank Sweeney Chief Information Officer AZDCS