



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
Security Awareness Training and Education Policy	DCS 05-8210	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	March 07, 2024	4

I. POLICY STATEMENT

The purpose of this policy is to ensure all DCS employees and contractors are appropriately trained and educated on how to fulfill their information security responsibilities. 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, 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 IT PSPs;
3. promote efforts within DCS to establish and maintain effective use of DCS information systems and assets;
4. promote security awareness training and education efforts within DCS.

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;
3. ensure security awareness training and educational material is periodically reviewed and updated to reflect changes in requirements, responsibilities, and changes to information security threats, techniques, or other relevant

aspects;

4. ensure those taking security awareness training and educational program have an effective way to provide feedback.

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 IT PSPs;
3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems;
4. ensure the development of an adequate security awareness training and education program for DCS;
5. coordinate the security awareness training and education program for DCS;
6. ensure all DCS personnel understand their responsibilities with respect to security awareness training and education;
7. stay informed in the security community by establishing contact with selected groups and associations within the security community to facilitate training, and maintain currency with recommended practices, and techniques.

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. Security Awareness Program Development

The DCS CISO or assigned delegate shall define, document, and develop a security awareness training and education program for DCS. The security training awareness and education program shall include the following elements:

1. Identifying Sensitive Positions - Identification of positions, systems, and applications with significant information security responsibilities, and identification of specialized training required to ensure personnel assigned to these positions, or having access to these systems and/or applications, are appropriately trained [HIPAA 164.308(a)(5)(i)].

This training shall include Role-based Security Training that contains appropriate content based on specific information security-related assigned roles and responsibilities [NIST 800 53 AT-3 supplemental guidance]. Roles that may require role-based training include DCS senior leaders or management officials.

Privacy training shall be provided with initial and annual training and include training in the employment and operation of personally identifiable information processing and transparency controls. [NIST 800-53 AT-3(5)]

2. DCS shall provide training to each member of the workforce.
3. Security training granted access to confidential information shall include all of the topics listed under section VI.B.3.a of this policy.
4. Security topics – Coverage of information security topics and techniques sufficient to ensure trained personnel comply with information security PSPs.
5. Periodic Security Reminders - Communication with employees and contractors providing updates to relevant information security topics or PSPs [HIPAA 164.308(a)(5)(ii)(A)].

B. Security Awareness Program Operations

The operations of the security training awareness and education program shall implement the following objectives:

1. Basic Security Awareness Training - All employees and contractors shall

complete security awareness training prior to being granted access to DCS information systems, when required by information system changes [NIST 800-53 AT-2 b], and at least annually thereafter [NIST 800-53 AT-2 a, c];

2. Basic Privacy Training - All employees and contractors shall complete privacy awareness training on the policies and procedures with respect to Personally Identifiable Information (PII) prior to being granted access to such data and upon a material change in the policies and procedures [HIPAA 164.530(b)]. All individuals responsible for handling consumer inquiries about the DCS's privacy practices or DCS's compliance with privacy regulations shall be informed of all the requirements in these regulations and how to direct consumers to exercise their rights under these regulations.
3. Specialized Security Awareness (SSA) Training - All employees and contractors shall receive relevant specialized training within 60 days of being granted access to DCS information systems.
 - a. DCS shall establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees granted access to confidential information.
 - b. Training shall include discussion of:
 - i. the sensitivity of confidential information and address the Privacy Act and other Federal and State laws governing its use and misuse;
 - ii. rules of behavior concerning use of and security in systems processing confidential data;
 - iii. restrictions on viewing and/or copying confidential information;
 - iv. the employee's responsibility for proper use and protection of confidential information including its proper disposal;
 - v. security incident reporting procedures;
 - vi. the possible sanctions and penalties for misuse of confidential information;
 - vii. basic understanding of procedures to protect the network

- from malware attacks;
- viii. spoofing, phishing and pharming scam prevention;
 - ix. social engineering and mining - provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining;
 - x. insider threats, including information on how these threats affect DCS systems.
4. DCS shall provide security awareness training annually or as needed and have in place administrative procedures for sanctioning employees up to and including termination who violate laws governing the use and misuse of confidential data through unauthorized or unlawful use or disclosure of confidential information.
- a. Each user is required to sign an electronic version of the DCS affirmation statement (terms and conditions for use) after reviewing the CBT and their agreement is captured and stored in a training database.
 - b. The User Affirmation Statement includes references to state and federal law and sanctions that include dismissal and/or prosecution.
5. Security Responsibilities - All employees and contractors shall be trained and educated in their information security responsibilities.
6. Acceptable Use Rules – all employees and contractors shall understand the acceptable use requirements of DCS information system, available technical assistance, and technical security products and techniques.
7. Training Material - Information security awareness training and education material shall be developed, available for timely delivery, and generally available to all DCS employees and contractors.
8. Training Delivery – Security awareness training and educational material shall be delivered in an effective manner.
9. Training techniques - DCS shall employ the DCS-defined techniques (e.g., displaying posters, privacy reminders, awareness events, email advisories) to increase the security and privacy awareness of system users. [NIST

800-53 AT-2.b]

C. Security Awareness Program Management and Maintenance

The DCS CISO or assigned delegate shall manage and maintain the security awareness training and education program. The security training awareness and education program management and maintenance activities shall include the following elements:

1. Tracking – DCS shall have effective tracking of security awareness training and education compliance for all employees and contractors with access to DCS information systems which includes periodic refresher training and education [NIST 800 53 AT-4]. Training records shall be retained for three years [NIST 800 53 AT-4 supplemental guidance]. However, DCS must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding, or exacting.
2. Acknowledgement – All employees or contractors who complete security awareness training and education programs shall acknowledge and accept that they have read and understand the DCS information system requirements around information security policy and procedures.
3. Program Updates – The security awareness training and education program shall be periodically reviewed and updated to reflect changes to information security threats, techniques, requirements, responsibilities, and changes to the rules of the system.
4. Security Groups and Associations – The DCS CISO or assigned delegate shall stay informed in the security community by establishing contact with selected groups and associations within the security community to facilitate training, and maintain currency with recommended practices and techniques [NIST 800 53 AT-5].
5. Feedback – the DCS CISO shall ensure that an appropriate mechanism exists for feedback to the quality and content of the security awareness training and education program.
 - a. Attendee Review of Security Awareness Training – All employees or contractors who complete security awareness training and educational programs shall have an effective way to provide feedback. Contact information shall be made available to provide

feedback at any time.

- b. Lessons Learned – Lessons learned from incident response and investigations shall drive improvements to the security awareness training and education program where relevant.

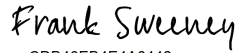
VII. DEFINITIONS

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 17	Initial Release	1	DeAnn Seneff
02 Jul 18	Annual Review	2	DeAnn Seneff
28 Mar 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-06 to DCS 05-8210 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	Robert Navarro
07 Mar 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	<p>DocuSigned by:  <small>CDB46EB4E4A6442...</small> 3/13/2024</p> <p>Frank Sweeney Chief Information Officer AZDCS</p>

