	STATEWIDE **POLICY**	**State of Arizona**

STATEWIDE POLICY (8210): SECURITY AWARENESS TRAINING AND EDUCATION

DOCUMENT NUMBER:	**P8210**
EFFECTIVE DATE:	**January 16, 2024**
REVISION:	**4.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this policy is to ensure all agency employees and contractors are appropriately trained and educated on how to fulfill their information security responsibilities.

3. SCOPE

3.1 Application to Budget Unit (BU) - This policy shall apply to all BUs as defined in ARS § 18-101(1).

3.2 Application to Systems - This policy shall apply to all agency system:

- **a. (P)** Policy statements preceded by "(P)" are required for agency system categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency system with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency system with protected healthcare information..
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency system with federal taxpayer information.

3.2 Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.2 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of Information Security PSPs throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the Director the risk to the state system and data based on current implementation of security controls and the mitigation options to improve security.

d. Provide a model for the implementation of security awareness training; and

e. Review and approve BU security training plans.

5.3 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Security PSPs;

b. Ensure BU compliance with security awareness training and education requirements, including training and education of personnel with significant information security responsibilities; and

c. Promote security awareness training and education efforts within the BU.

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of Information Security PSPs;

b. 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; and

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

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Information Security PSPs;

b. Ensure the development of an adequate security awareness training and education program for the BU;

c. Coordinates the security awareness training and education program for BU;

d. Ensure all personnel understand their responsibilities with respect to security awareness training and education; and

e. 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.

5.7 Supervisors of agency employees and contractors shall:

- **a.** Ensure users are appropriately trained and educated on their information security responsibilities; and
- **b.** Monitor employee activities to ensure compliance.

5.8 Users of agency system shall:

- **a.** Familiarize themselves with this policy and related PSPs; and
- **b.** Adhere to PSPs regarding security awareness training and education.

6. STATEWIDE POLICY

6.1 Security Awareness Program Development - The BU ISO or assigned delegate shall define, document, and develop a security awareness training and education program for the BU. The security training awareness and education program shall include the following elements: [PCI DSS 12.6]

6.1.1 (P) **Identify 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)]

- **a.** The BU shall provide role-based security and privacy training to those assigned security and privacy roles and responsibilities prior to being authorized access to the system, information, or performing assigned duties, and when required by system changes. [NIST 800-53 AT-3.a].
- **b.** (P) 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)]

6.1.2 The BU shall provide training to each member of the workforce.

6.1.3 (P-FTI) Security training granted access to SSA-provided information shall include all of the topics listed in 6.2.3.a.

6.1.4 **(P-PCI) Payment Card Capture Device Training** - For personnel working in areas with payment card data capture devices, the BU shall provide training for personnel to be aware of attempted tampering or replacement of devices. Training shall include: [PCI DSS 9.9, 9.9.3]

a. verification of identity of third party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices

b. verification procedures to installation, replacement, or device returns

c. being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices)

d. reporting procedures for suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)

6.1.5 **Security Topics** - Coverage of information security topics and techniques sufficient to ensure trained personnel comply with information security PSPs.

6.1.6 (P) **Periodic Security Reminders** - Communication with employees and contractors providing updates to relevant information security topics or PSPs. [HIPAA 164.308(a)(5)(ii)(A)]

6.2 Security Awareness Program Operations – The BU ISO or assigned delegate shall operate the security awareness training and education program for the BU. The operations of the security training awareness and education program shall implement the following objectives:

6.2.1 **Security and Privacy Literacy Training and Awareness** - All employees and contractors shall complete security and privacy literacy training prior to being granted access to agency system, when required by information system changes [NIST 800-53 AT-2 b], and at least annually thereafter. [PCI 12.6.1, NIST 800-53 AT-2.a]

a. Insider Threat - Security and privacy literacy training and awareness shall include training on recognizing and reporting potential indicators of insider threat. [NIST 800-53 AT-2(2)]

b. Social Engineering and Mining - Security and privacy literacy training and awareness shall include training on recognizing and reporting potential and actual instances of social engineering and social mining. [NIST 800-53 AT-2(3)]

c. Rules of Behavior - Security and privacy literacy training and awareness shall include training on the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy. See P8120: Information System Security Program. [NIST 800-53 PL-4]

6.2.2 (P) **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)]

d. (P) Privacy Training – All individuals responsible for handling consumer inquiries about the BU's privacy practices or the BU'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.

6.2.3 **Specialized Security Awareness Training** - All employees and contractors shall receive relevant specialized training within 60 days of being granted access to agency system.

a. (P-FTI) The BU shall establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees granted access to SSA-provided information. Training shall include discussion of:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and State laws governing its use and misuse;
- Rules of behavior concerning use of and security in systems processing SSA-provided data;
- Restrictions on viewing and/or copying SSA-provided information;
- The employee's responsibility for proper use and protection of SSA-provided information including its proper disposal;
- Security incident reporting procedures;
- The possible sanctions and penalties for misuse of SSA-provided information;
- Basic Understanding of procedures to protect the network from malware attacks; and
- Spoofing, phishing and pharming scam prevention.

e. (P-FTI) The BU 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 SSA-provided data through unauthorized or unlawful use or disclosure of SSA-provided information.

- Each user is required to sign an electronic version of the ADOA affirmation statement (terms and conditions for use) after reviewing the CBT and their agreement is captured and stored in a database.

- The User Affirmation Statement includes reference to state and federal law and sanctions that include dismissal and/or prosecution.

6.2.4 **Security Responsibilities** - All employees and contractors shall be trained and educated in their information security responsibilities.

6.2.5 **Acceptable Use Rules** - All employees and contractors shall understand the acceptable use requirements of the agency information system, available technical assistance, and technical security products and techniques.

6.2.6 **Training Material** - Information security awareness training and education material shall be developed, available for timely delivery, and generally available to all agency employees and contractors.

6.2.7 **Training Delivery** - Security awareness training and educational material shall be delivered in an effective manner.

a. Training techniques - The BU shall employ the BU-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]

6.3 Security Awareness Program Management and Maintenance - The BU ISO or assigned delegate shall manage and maintain the security and privacy training and awareness program for BU. The security and privacy training and awareness program management and maintenance activities shall include the following elements:

6.3.1 **Tracking** - The BU shall document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training. [NIST 800-53 AT-4.a]

a. Training Record Retention - Individual training records shall be retained for three years. [NIST 800-53 AT-4.b] 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 and https://apps.azlibrary.gov/records/general_rs/GS-1006.pdf Record Series Number 10311-10312.

6.3.2 **Acknowledgement** - All employees or contractors who complete security awareness training and education programs shall acknowledge and accept that they have read and understand the agency information system requirements around information security policy and procedures. [PCI 12.6.2]

6.3.3 **Program Updates** - The security and privacy literacy training and awareness program and any additional security and privacy role-based training shall be

periodically reviewed and updated to reflect changes to information security and privacy threats, techniques, requirements, responsibilities, and changes to the rules of the system. [NIST 800-53 AT-2.c, AT-3.b]

6.3.4 **Feedback** - The BU ISO shall ensure 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 internal or external security and privacy incidents or breaches shall be incorporated into the security and privacy literacy training and awareness and security and privacy role-based training techniques and content. [NIST 800-53 AT-2.d, AT-3.d]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8210 Security Awareness Training and Education

8.2 Statewide Policy Exception Procedure

8.3 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

8.4 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.5 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 ,PCI Security Standards Council, May 2018.

8.6 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

8.7 General Records Retention Schedule for All Public Bodies, Administrative Records, Schedule Number 000-12-15, Arizona State Library, Archives and Public Records, Item Number 25

8.8 General Records Retention Schedule for All Public Bodies, Human Resources / Personnel Records, Schedule Number GS 1006, Arizona State Library, Archives and Public Records, Item Number 12

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
9/01/2014	**Initial release**	**Draft**	**Aaron Sandeen, State CIO and Deputy Director**
10/11/2016	**Updated all the Security Statutes**	**1.0**	**Morgan Reed, State CIO and Deputy Director**
9/17/2018	**Updated for PCI-DSS 3.2.1**	**2.0**	**Morgan Reed, State of Arizona CIO and Deputy Director**
5/26/21	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer**
1/16/2024	**Annual Updates**	**4.0**	Ryan Murray (Jan 16, 2024 17:06 MST) **Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

P8210_Security_Awareness_Training_And_Education (1)

Final Audit Report 2024-01-17

Created:	2024-01-16
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAA-QwTdmMkkhVPnroHHQLstVySdCKL_aHF

"P8210_Security_Awareness_Training_And_Education (1)" History

Document created by Ed Yeargain (eyeargain@azdohs.gov)
2024-01-16 - 11:52:15 PM GMT

Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature
2024-01-16 - 11:52:57 PM GMT

Document e-signed by Ryan Murray (rmurray@azdohs.gov)
Signature Date: 2024-01-17 - 0:06:33 AM GMT - Time Source: server

Agreement completed.
2024-01-17 - 0:06:33 AM GMT