ARIZONA STATEWIDE SECURITY STANDARD	STATEWIDE STANDARD	State of Arizona

STANDARD 8210: SECURITY AWARENESS TRAINING AND EDUCATION

DOCUMENT NUMBER:	S8210
EFFECTIVE DATE:	JULY 1, 2015
REVISON:	DRAFT

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 18-105.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy, (P8210) requirements.

3. SCOPE

3.1 **Application to Budget Units** - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 **Application to Systems** - This policy shall apply to all state information systems. Policy statements preceded by “(P)” are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

3.3 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 subject matter experts shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

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

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology PSPs throughout all state BUs;

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

c. Review and approve BU security training plans; and

d. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Statewide Information Technology PSPs within the BU;

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.

5.4 BU Chief Information Officer (CIO) shall:

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

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.

5.5 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 Statewide Information Technology 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.

5.6 Supervisors of state 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.

5.7 Users of state information systems shall:

a. Familiarize themselves with this and related PSPs; and

b. Adhere to PSPs regarding security awareness training and education.

6. STATEWIDE POLICY

6.1 Security Awareness Program Development - To be effective security awareness training and education needs to be focused on the entire user population including senior management and the various roles within the BU.

6.1.1 (P) Identify Sensitive Positions - The BU shall identify roles with significant responsibility for information security. *Note: Table 1 is provided as an example.*

Roles	
• Business Unit Head and Other Executives	• Assessor
• Chief Information Officer	• External Auditor, Internal Auditor
• Information Security Officer	• Contracting Officer
• Privacy Officer	• Database Administrator
• Data Center Manager	• Network Administrator
• Incident Response Coordinator	• Programmer / System Analyst
• Director of Information Technology	• Security Administrator
• General Council	• Systems Administrator
• Functional Managers	• System Owner
• Risk Manager	• Technical Support Personnel

Table 1. Typical BU Security Roles - *Each BU implementing role-based security training shall document the associated BU roles with security responsibilities*

6.1.2 (P) Role-based Security Training - The BU shall provide security training, with the appropriate content, based on specific information security related assigned roles and responsibilities as described in Table 1.

An example of a role based training method is outlined in the NIST 800-16 standard. This standard identifies both organizational responsibilities and training areas, which are assigned for each of the identified organizational roles. This NIST approach to role based training creates a training matrix for each of the identified roles to assign the educational topics required for each role. Examples of role-based training matrices are provided in Table 2:

Role: Business Unit Head or Other Executives					
	Responsibilities				
Training Areas	**Manage**	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations					X
Security Program					
Planning					X
Management					X
System Life Cycle Security					
Initiation					X
Development/Acquisition					X
Implementation/Assessment					X
Operations/Maintenance					X
Disposal					X

Table 2. Role-Based Training Matrices - BUs implementing role-based security training shall document the training objectives and security topics appropriate for each identified role. These role-based training matrices are an example of allocating security topics based on the role and their responsibilities in the five general areas of organizational responsibility: Manage, Acquire, Design and Develop, Implement and Operate, and Review.

For the identified roles in this example the following training matrices are completed:

Role: Chief Information Officer					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations	X				
Security Program					
Planning	X		X	X	X
Management	X		X	X	X
System Life Cycle Security					
Initiation					
Development/Acquisition					
Implementation/Assessment				X	
Operations/Maintenance				X	
Disposal					

Role: Information Security Officer					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations	X	X	X	X	X
Security Program					
Planning	X	X	X	X	X
Management	X	X	X	X	X
System Life Cycle Security					
Initiation	X	X	X	▨	X
Development/Acquisition	X	X	X	X	X
Implementation/Assessment	X	X	X	X	X
Operations/Maintenance	X	X	X	X	X
Disposal	X	▨	▨	X	X

Role: Privacy Officer					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations					
Security Program					
Planning					
Management					
System Life Cycle Security					
Initiation					
Development/Acquisition			X		
Implementation/Assessment					
Operations/Maintenance					
Disposal				X	

Role: Data Center Manager					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations					
Security Program					
Planning					
Management					
System Life Cycle Security					
Initiation					
Development/Acquisition				X	
Implementation/Assessment				X	
Operations/Maintenance	X			X	
Disposal	X			X	

Role: Incident Response Coordinator					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations				X	
Security Program					
Planning			X	X	
Management				X	
System Life Cycle Security					
Initiation					
Development/Acquisition					
Implementation/Assessment					
Operations/Maintenance				X	
Disposal					

Role: Director of Information Technology

Training Areas	Responsibilities				
	Manage	Acquire	Design & Develop	Implement & Operate	Review & Evaluate
Laws & Regulations	X		X		X
Security Program					
Planning	X	X	X	X	
Management	X	X	X	X	
System Life Cycle Security					
Initiation	X				X
Development/Acquisition	X				
Implementation/Assessment	X				
Operations/Maintenance					
Disposal					X

Role: General Council

Training Areas	Responsibilities				
	Manage	Acquire	Design & Develop	Implement & Operate	Review & Evaluate
Laws & Regulations	X	X	X	X	X
Security Program					
Planning				X	X
Management				X	X
System Life Cycle Security					
Initiation					X
Development/Acquisition					X
Implementation/Assessment					X
Operations/Maintenance					X
Disposal					X

Role: Organizational Unit Manager

Training Areas	Responsibilities				
	Manage	Acquire	Design & Develop	Implement & Operate	Review & Evaluate
Laws & Regulations			X		
Security Program					
Planning	X				
Management	X			X	
System Life Cycle Security					
Initiation	X		X		
Development/Acquisition					X
Implementation/Assessment	X	X	X		X
Operations/Maintenance	X	X			
Disposal	X			X	

Role: Risk Manager					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations					X
Security Program					
Planning					X
Management					X
System Life Cycle Security					
Initiation					X
Development/Acquisition					X
Implementation/Assessment					X
Operations/Maintenance					X
Disposal					X

Role: Assessor / Internal/External Auditor					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations			X		X
Security Program					
Planning				X	X
Management				X	X
System Life Cycle Security					
Initiation					X
Development/Acquisition			X		X
Implementation/Assessment			X		X
Operations/Maintenance					X
Disposal					X

Role: Contracting Officer					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations		X			
Security Program					
Planning		X			
Management		X			
System Life Cycle Security					
Initiation		X			
Development/Acquisition		X			
Implementation/Assessment		X			
Operations/Maintenance		X			
Disposal		▨			

Role: Database / Network / Security Administrator					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations				X	
Security Program					
Planning				X	
Management				X	
System Life Cycle Security					
Initiation					
Development/Acquisition				X	
Implementation/Assessment			X	X	
Operations/Maintenance	X		X	X	
Disposal				X	

Role: Programmer / Systems Analyst					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations			X	X	
Security Program					
Planning					
Management					
System Life Cycle Security					
Initiation				▨	
Development/Acquisition			X	X	
Implementation/Assessment			X	X	
Operations/Maintenance			X	X	
Disposal			▨	X	

Role: System Owner					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations					
Security Program					
Planning	X			X	
Management				X	
System Life Cycle Security					
Initiation	X	X	X		X
Development/Acquisition	X				X
Implementation/Assessment	X	X			X
Operations/Maintenance	X	X			
Disposal	X	▨			

Role: Technical Support Personnel					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations				X	
Security Program					
Planning					
Management					
System Life Cycle Security					
Initiation				X	
Development/Acquisition				X	
Implementation/Assessment				X	
Operations/Maintenance				X	
Disposal				X	

BUs using the matrices approach above should provide training corresponding to each of the matrices cells to the roles within the agency. Modular training provides for flexibility in the availability and delivery of training. The content of such training should meet the behavioral outcomes in the following table. For additional information refer to the NIST SP 800-16 guideline.

Information Security Behavioral Outcomes					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
Laws & Regulations	Managers are able to understand applicable governing documents and interpret and apply them to the manager's responsibility area.	IT acquisition professionals have a sufficient understanding of information security requirements and issues to protect the government's interest in such acquisitions.	AIS design and development professionals are able to translate IT laws and regulations into technical specifications to provide adequate and appropriate levels of protection.	AIS operations professionals are able to understand information security laws and regulations in sufficient detail to ensure that appropriate safeguards are in place and enforced.	AIS assessors are able to use information security laws and regulations in developing a comparative baseline and determining the level of system compliance.
Security Program					
Planning	Managers are able to understand principles and processes of program planning and can organize resources to develop a security program that meets organizational needs.	Information security planning professionals can identify the resources required for successful implementation. Individuals recognize the need to include information security requirements in IT acquisitions and to incorporate appropriate acquisition policy and	Information security program design and development professionals are able to create a security program plan specific to a business process or organizational entity.	Information security operations professionals are able to develop plans for security controls, countermeasures, and processes as required to execute the existing program.	Information security program assessors are able to review the program to determine its continuing capability to cost-effectively address identified requirements.

Information Security Behavioral Outcomes					
Training Areas	**Responsibilities**				
	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**
		oversight in the information security program.			
Management	Information security program managers understand how (and are able) to implement a security program that meets their organization's needs.	Information security program managers have a sufficient understanding of information security and the acquisition process to incorporate information security program requirements into acquisition work steps.	Information security program design and development professionals have sufficient understanding of the appropriate program elements and requirements to be able to translate them into detailed policies and procedures, which provide adequate and appropriate protection for the organization's IT, resources in relation to acceptable levels of risk.	Information security operations professionals have a sufficient understanding of the appropriate program elements and requirements to be able to apply them in a manner which provides adequate and appropriate levels of protection for the organization's IT resources.	Information security program assessors have an adequate understanding of information security laws, regulations, standards, guidelines, and the organizational environment to determine if the program adequately addresses all threats and areas of potential vulnerability.

System Life Cycle Security					
Initiation	Managers are able to identify steps in the system development life cycle where security requirements and concerns (e.g., confidentiality, integrity, and availability) need to be considered and to define the processes to be used to resolve those concerns.	Acquisition professionals are able to analyze and develop acquisition documents and/or provide guidance which ensures that functional information security requirements are incorporated.	System design and development professionals are able to translate information security requirements into system- level security specifications.		IT Assessors are able to evaluate planning documents associated with a particular system to ensure that appropriate information security requirements have been considered and incorporated.
Development / Acquisition	Managers are able to ensure that the formal developmental baseline includes approved security requirements and that security-related features are installed, clearly identified, and documented.	Acquisition professionals are able to monitor procurement actions to ensure that information security requirements are satisfied.	System design and development professionals are able to use baseline information security requirements to select and install appropriate safeguards.	System operators are able to assemble, integrate, and install systems so that the functionality and effectiveness of safeguards can be tested and evaluated.	IT Assessors are able to examine development efforts at specified milestones to ensure that approved safeguards are in place and documented.
Implementation /Assessment	Managers are able to oversee the implementation and deployment of an IT system in a manner that does not compromise in-place and tested security safeguards.	Acquisition professionals are able to ensure that the system, as implemented, meets all contractual requirements related to the security and privacy of IT resources.	System design and development professionals are able to participate in the development of procedures which ensure that safeguards are not compromised as they are incorporated into the production environment.	System operators ensure that approved safeguards are in place and effective as the system moves into production.	IT Assessors are able to analyze system and test documentation to determine whether the system provides adequate and appropriate information security to support certification and accreditation.

Operations / Maintenance	Managers are able to monitor operations to ensure that safeguards are effective and have the intended effect of balancing efficiency with minimized risk.	Acquisition professionals are able to understand the information security concerns associated with system operations and to identify and use the appropriate contract vehicle to meet current needs in a timely manner.	System design and development professionals are able to make procedural and operational changes necessary to maintain the acceptable level of risk.	System operators are able to maintain appropriate safeguards continuously within acceptable levels of risk.	IT Assessors are able to examine the operational system to determine the adequacy and effectiveness of safeguards and to ensure that a consistent and appropriate level of security (i.e., one with an acceptable level of risk) is maintained.
Disposal	Managers are able to understand the special information security considerations and measures required during the shutdown of a system, and effectively plan and direct these activities.			System operators are able to develop and implement the system termination plan, including security requirements for archiving/disposing of resource.	IT Assessors are able to verify the appropriateness of the disposal plan and processes used to dispose of the IT system securely.

Table 3. Security Training Outcomes by Responsibility and Training Area - This table documents the behavioral outcomes for training modules designed for various roles within the BU.

6.1.3 Security Topics - The BU shall determine the appropriate set of security topics to cover in security awareness training. The set of security topics relevant for a specific BU may differ based on mission, environment, threats, assets, and user population. The following set of security awareness topics should be modified to meet the needs of the BU.

Topic	Description
Password usage & management	Minimum complexity requirements, creation, frequency of changes, lost password procedures, and protection of password.
Protection from viruses, worms, Trojan horses, and other malicious code	Systematic scanning, and updating of signature definitions
Policy	Implications of noncompliance on user and BU
Unknown email/attachments	Recognizing malicious email and dangers on clicking links or downloading attachments.
Web usage	Allowed versus prohibited; BU monitoring of user activity.
Spam	Definition of spam, reporting abuse.
Data backup and storage	Centralized or decentralized approach
Social engineering	Definition and protection from.
Incident response	Contacts, responsibility in reporting.
Shoulder surfing	Definition, dangers, how to protect from.
Changes in system environment	Increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
Inventory and property transfer	Identify responsible organization and user responsibilities (e.g., media sanitization)
Personal use and gain issues	Systems at work and home
Handheld device security issues	Address both physical and wireless security issues
Use of encryption	Transmission of sensitive/confidential information over the Internet. Address BU policy, procedures, and technical contact for assistance
Laptop security while on travel	Address both physical and information security issues
Personally owned systems and software at work	State whether allowed or not (e.g., copyrights)
Timely application of system patches	Role in configuration management
Software license restriction issues	Address when copies are allowed and not allowed
Supported/allowed software on organization systems	Role in configuration management
Access control issues	Address least privilege and separation of duties
Individual accountability	Explain what this means in the organization
Use of acknowledgement statements	Passwords, access to systems and data, personal use and gain
Visitor control and physical access to spaces	Discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
Desktop security	Discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
Protect information subject to confidentiality concerns	In systems, archived, on backup media, in hardcopy form, and until destroyed
Email list etiquette	Attached files and other rules

Table 4. Sample set of security topics

6.1.4 **(P) Periodic security reminders –** The BU shall implement appropriate techniques to communicate information security training throughout the year to all employees. The appropriate technique(s) used to disseminate the message throughout the BU depends on the available resources of the BU for training and the complexity of the message. The following techniques are provided as examples:

a. Messages on awareness tools (e.g., pens, key fobs, post-it notes, notepads, first aid kits, clean-up kits, USB drives, bookmarks, other tchotchkes),

b. Posters, "do and don't lists," or checklists,

c. Screensavers and warning banners/messages,

d. Newsletters,

e. Desk-to-desk alerts (e.g., a hardcopy, bright-colored, one-page bulletin) – either one per desk or routed through an office – that is distributed through the organization's mail system)

f. Agency wide email messages,

g. Videotapes,

h. Web-based sessions,

i. Computer-based sessions,

j. Teleconferencing sessions,

k. In-person, instructor-led sessions, IT security days or similar events,

l. Lunch & Learn or "Brown bag" seminars,

m. Pop-up calendar with security contact information, monthly security tips, etc. and/or

n. Awards program (e.g., plaques, mugs, letters of appreciation)

6.2 **Security Awareness Program Operations** - The BU ISO or assigned delegate operates the security awareness training and education program for BU. The operations of the security training awareness and education program implements the following objectives:

6.2.1 **Basic Security Awareness Training** - All employees and contractors complete security awareness training prior to being granted access to state information systems, when required by information system changes [NIST 800-53 AT-2 b], and least annually thereafter. [PCI 12.6.1, NIST 800-53 AT-2 a, c]

6.2.2 **(P) Basic Privacy Training** - All employees and contractors 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)]

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

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

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

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

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

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA website.

8. REFERENCES

8.1 Policy 8210, Security Awareness Training and Education

8.2 NIST 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

8.3 NIST 800-16, Information Security Training Requirements: A role- and Performance-Based Model (Draft), March 2009.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director