STATEWIDE

POLICY

State of Arizona

STATEWIDE POLICY (8130): SYSTEM SECURITY ACQUISITION AND DEVELOPMENT

DOCUMENT NUMBER:	**P8130**
EFFECTIVE DATE:	**JANUARY 30, 2025**
REVISION:	**5.0**

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 establish adequate security controls for the acquisition and deployment of agency systems.

3. SCOPE

3.1 **Application to Budget Units (BUs)** - 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 agency systems:

a. **(P)** Policy statements preceded by "(P)" are required for agency systems categorized as protected.

b. **(P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency systems with payment card industry data (e.g., cardholder data).

c. **(P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency systems with protected healthcare information.

d. **(P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency systems with federal taxpayer information.

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 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 statewide information security PSPs throughout all state budget units (BUs).

5.2 State Chief Information Security Officer (CISO) shall:

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

b. Review and approve all state agency BU security and privacy PSPs;

c. Request exceptions from the statewide security and privacy PSPs; and

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

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 Budget Unit (BU) Director shall:

b. Be responsible for the correct and thorough completion of BU PSPs;

c. Ensure compliance with BU PSPs; and

d. Promote efforts within the BU to establish and maintain effective use of agency systems and assets.

5.5 BU Chief Information Officer (CIO) shall:

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

b. Ensure PSPs are periodically reviewed and updated to reflect changes in requirements.

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 BU statewide information security PSPs;

b. Ensure the development and implementation of adequate controls enforcing the System Security Acquisition Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to secure acquisition of agency systems and components.

5.7 BU Procurement Official shall:

a. Provide advice and support with the procurement of goods and services in regards to request for information, request for proposal, evaluation of response, and contract awards; and

b. Ensure compliance with Arizona procurement statutes and PSPs throughout the procurement process.

5.8 Purchaser shall:

a. Abide by all PSPs throughout the procurement process.

6. (AGENCY) POLICY

6.1 **Allocation of Resources** - The BU shall: [NIST 800 53 SA-2]

a. Determine the high-level information security and privacy requirements for the agency system or system service in mission/business process planning;

b. Determine, document and allocate the resources required to protect the agency system or system service as part of its capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

6.2 Technology Life cycle - The BU shall: [NIST 800 53 SA-3]

a. Manage the agency system using a BU-defined technology life cycle that is based on industry standards or best practices and incorporates information security considerations; [PCI DSS 6.3]

b. Define and document information security and privacy roles and responsibilities throughout the technology life cycle;

c. Identify individuals having information security roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into technology life cycle activities.

6.2.1 **Software Development Process** - The BU shall require developers of agency systems or system components to implement the following software development processes: [PCI DSS 6.3]

a. Remove non-production application accounts, user IDs, and passwords before applications become active or are released to customers; and [PCI DSS 6.3.1]

b. Review custom code prior to release to production or customers in order to identify any potential coding vulnerabilities. Review shall be performed by someone other than the code author and by someone knowledgeable of code review techniques and secure coding practices; based on secure coding guidelines; and reviewed and approved by management. [PCI DSS 6.3.2]

6.2.2 (P) **Change Control Procedures** - The BU shall require developers of agency systems, or system components to follow change control processes and procedures for all changes to system components. The process must ensure: [PCI DSS 6.4.3]

a. Ensure separate development/test and production environments; [PCI DSS 6.4.1]

b. Ensure separation of duties between development/test and product environments; [PCI DSS 6.4.2]

c. Ensure production data is not used for testing or development; [PCI DSS 6.5.5]

d. Ensure removal of test data and accounts before production systems become active; [PCI DSS 6.4.4]

e. Include documentation of the impact; [PCI DSS 6.4.5.1]

f. Include documented change approval by authorized parties; [PCI DSS 6.4.5.2]

g. Include functionality testing to verify that the change does not adversely impact the security of the system; [PCI DSS 6.4.5.3]

h. Include back-out procedure; and [PCI DSS 6.4.5.4]

i. Upon completion of a significant change, all relevant security requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. [PCI DSS 6.4.6]

6.2.3 (P) **Secure Coding Guidelines** - The BU shall require developers of agency systems, or system components, to develop applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes, to include the following: [PCI DSS 6.5]

- BU shall ensure passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. [PCI DSS 8.6.2]

a. Injection flaws, particularly SQL injection (also consider OS Command Injection, LDAP and XPath injection flaws, as well as other injection flaws); [PCI DSS 6.5.1]

b. Buffer overflow; [PCI DSS 6.5.2]

c. Insecure cryptographic storage; [PCI DSS 6.5.3]

d. Insecure communications; [PCI DSS 6.5.4]

e. Improper error handling; [PCI DSS 6.5.5]

f. All “High” vulnerabilities identified in the vulnerability identification process; and [PCI DSS 6.5.6]

g. For web applications and web application interfaces:

1. Cross-site scripting (XSS) [PCI DSS 6.5.7]

2. Improper Access Control (such as direct object references, failure to restrict URL access, and directory traversal) [PCI DSS 6.5.8]

3. Cross-site request forgery (CSRF) [PCI DSS 6.5.9]

4. Broken authentication and session management. [PCI DSS 6.5.10]

6.3 Acquisition Process - The BU shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: [NIST 800 53 SA-4]

a. Security and privacy functional requirements;

b. Security strength requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements;

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

6.3.1 (P) **Functional Properties of Security Controls** - The BU shall require the developer of the agency system, system component, or system service to provide a description of the functional properties of the controls to be employed. [NIST 800 53 SA-4(1)] [IRS Pub 1075]

6.3.2 (P) **Design/Implementation Information for Security Controls** - The BU shall require the developer of the agency system, system component, or agency system service to provide design and implementation information for the controls to be employed that includes: [NIST 800 53 SA-4(2)] [IRS Pub 1075]

a. Security-relevant external system interfaces; and

b. High-level design.

6.3.3 (P) **Services in Use** - The BU shall require the developer of the agency system component, or agency system service to identify the functions, ports, protocols, and services intended for organizational use. [NIST 800 53 SA-4(9)] [IRS Pub 1075]

6.3.4 (P) **Use of Approved PIV Products** - The BU shall employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within BU systems. [NIST 800-53 SA-4(10)]

6.4 State system Documentation - The BU shall: [NIST 800 53 SA-5]

a. Obtain or develop administrator documentation for the agency system, system component, or agency system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security functions/mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions.

b. Obtain or develop user documentation for the agency system, system component, or agency system service that describes:

1. User-accessible security and privacy functions/mechanisms and how to effectively use those functions and mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy;
3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Ensure documentation is available to BU-defined personnel or roles

6.5 (P) **Security Engineering Principles** - The BU shall apply system security and privacy engineering principles in the specification, design, development, implementation, and modification of the agency systems and system components. [NIST 800 53 SA-8] [IRS Pub 1075]

6.6 (P) **Personally Identifiable Information Minimization** - The BU shall implement the privacy principle of minimization using BU-defined processes. [NIST 800-53 SA-8(33)]

6.7 **External system Services** - The BU shall: [NIST 800 53 SA-9]

a. Require that providers of external agency system services comply with organizational information security and privacy requirements and employ security controls in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
c. Employ Service Level Agreements (SLAs) to monitor control compliance by external service providers on an ongoing basis. [HIPAA 164.308(b)(1), 164.314(a)(2)(i)]

6.7.1 **Identification of Services** - The BU shall require providers of external system services to identify the functions, ports, protocols, and other services required for the use of such services. [NIST 800 53 SA-9(2)] [IRS Pub 1075]

6.7.2 **(P-FTI) Processing, Storage, and Service Location** - The BU shall restrict the location of systems that receive, process, store, or transmit confidential information to areas within the United States territories, embassies, or military installations. [NIST 800-53 SA-9(5)] [IRS Pub 1075]

6.8 (P) **Develop Configuration Management** - The BU shall require the developer of the system, system component, or system service to: [NIST 800 53 SA-10] [IRS Pub 1075]

a. Perform configuration management during system, component, or service (development, implementation, and operation);

b. Document, manage, and control the integrity of changes to configuration items under configuration management;

c. Implement only BU-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes, and;

e. Track security flaws and flaw resolution within the system, component, or service.

6.9 (P) **Develop Security Testing and Evaluation** - The BU shall require the developer of the system, system component, or system service at all post-design stages of the system development life cycle, to: [NIST 800 53 SA-11] [IRS Pub 1075]

a. Develop and implement a plan for ongoing security and privacy control assessments; perform integration and regression testing for components and services and unit, integration, and system testing for systems;

b. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

c. Implement a verifiable flaw remediation process; and

d. Correct flaws identified during security testing and evaluation.

6.9.1 (P) **Public Web Application Protections** - The BU shall require the provider of agency system service for public-facing web applications to address new threats and vulnerabilities on an ongoing basis and to ensure that these applications are protected against known attacks by either of the following methods: [PCI DSS 6.6]

a. Reviewing public-facing web applications using manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or

b. Installing a web-application firewall in front of public facing web applications.

6.9.2 (P) **Threat and Vulnerability Analyses** - The BU shall require the developer of the system, system component, or system service to perform threat modeling and vulnerability analysis during development and subsequent testing and evaluation of the system, component, or service that: [NIST 800 53 SA-11(2)] [IRS Pub 1075]

a. Uses the BU-defined contextual information concerning impact, environment of operations, known or assumed threats, and acceptable risks;

b. Employs BU-identified tools and methods;

c. Conducts the modeling and analyses at the BU-defined level of rigor; and

d. Produces evidence that meets the BU-defined acceptance criteria.

6.9.3 (P) **Independent Verification of Assessment Plans and Evidence** - The BU shall: [NIST 800 53 SA-11(3)] [IRS Pub 1075]

a. Require an independent agent to verify the correct implementation of the developer security and privacy assessment plan and the evidence produced during security testing and evaluation.

b. Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.

6.9.4 (P) **Penetration Testing and Analysis** - The BU shall require the developer of the agency system, system component, or agency system service to perform penetration testing to include black box testing by skilled security professionals simulating adversary actions and with automated code reviews. [NIST 800 53 SA-11(5)] [IRS Pub 1075] [PCI DSS 11.3.2]

6.10 Establish Operational Procedures – The BU shall ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. [PCI DSS 6.7]

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 EXCEPTION PROCEDURE

8.2 STATEWIDE POLICY FRAMEWORK P8130 SYSTEM SECURITY ACQUISITION AND DEVELOPMENT

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.

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
5/26/2021	Annual Updates	3.0	Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer
12/19/2023	Annual Updates	4.0	Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer
1/30/2025 2/11/2025	Annual Updates	5.0	Errika Celsy, Chief Privacy and Compliance Officer; Deputy Director Department of Homeland Security & State Chief Information Security Officer