	Statewide **POLICY**	**State of Arizona**

STATEWIDE POLICY (8110): DATA CLASSIFICATION

DOCUMENT NUMBER:	**(P8110)**
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 provide a framework for the protection of data that is created, stored, processed or transmitted STATEWIDE. The classification of data is the foundation for the specification of policies, procedures, and controls necessary for the protection of Confidential Data.

3. SCOPE

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

- **a.** (P) Policy statements preceded by "(P)" are required for BU systems categorized as Protected.
- **b.** (P-PCI)Policy statements preceded by "(P-PCI)" are required for BU systems with payment card industry data (e.g., cardholder data).
- **c.** (P-PHI) Policy statements preceded by "(P-PHI)" are required for BU systems with protected healthcare information.
- **d.** (P-FTI) Policy statements preceded by "(P-FTI)" are required for BU 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 subject matter experts 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 Statewide Chief Information Security Officer (CISO) shall:

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

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing PSPs; and

c. 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 Statewide 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 BU PSPs;

b. Ensure compliance with BU PSPs;

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

d. Be the data owner for all Confidential Data sets or shall delegate a data owner for each set of Confidential Data.

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT and information security PSPs; and

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

5.6 BU ISO shall:

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

b. Ensure the development and implementation of adequate controls enforcing the Statewide and BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to securing agency systems, including classification of data and handling.

5.7 Data Owner shall:

a. Assign classification of data;

b. Assign data custodians and ensure data custodian is familiar with the protection requirements for Confidential Data;

c. Participate in establishing, approving and maintaining policies for the protection of data within state agency; and

d. Promote data resource management within the state agency.

5.8 Data Custodian shall:

a. Ensure implementation of controls according to BU PSPs.

5.9 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.

5.10 System Users of agency systems shall:

a. Become familiar with this and related PSPs; and

b. Adhere to PSPs regarding classification of data and handling within agency systems.

6. STATEWIDE POLICY

6.1 **Data Classification** - Data created, stored, processed or transmitted on agency systems shall be classified according to the impact to the state or citizens resulting from the disclosure, modification, breach or destruction of the data.

6.2 **Data Classification Categories** - All agency data shall be classified as one of the following categories: [National Institute of Standards and Technology Special Publication (NIST SP) 800-53 RA-2]

6.2.1 **Confidential Data** - Data that shall be protected from unauthorized disclosure based on various laws, regulations, policies, and other legal agreements governing its protection. Examples of Confidential Data include:

a. System Security Parameters and Vulnerabilities

1. System security vulnerabilities

2. Generated security information

3. Information regarding current deployment, configuration, or operation of security products or controls

b. Health Information
- **1.** Protected Health Information [Health Insurance Portability and Accountability Act (HIPAA) - PL 104-191, Sections 261 - 264, 45 CFR Part 160 and 164]
- **2.** Medical records [A.R.S. 12-2291, A.R.S. § 12-2292, A.R.S 36-445.04, A.R.S. § 36-404, A.R.S. § 36-509, A.R.S. § 36-3805]
- **3.** Child immunization data [A.R.S. § 36-135]
- **4.** Chronic disease information [A.R.S. § 36-133]
- **5.** Communicable disease information [A.R.S. § 36-664, A.R.S. § 36-666]
- **6.** Developmental disabilities service records [A.R.S. § 36-568.01, A.R.S. § 36-568.02]
- **7.** Emergency medical service patient records [A.R.S. § 36-2220]
- **8.** Genetic testing records [A.R.S. § 12-2801, A.R.S. § 12-2802]
- **9.** Home health service records [A.R.S. § 36-160]
- **10.** Midwifery patient records [A.R.S. § 36-756.01]
- **11.** State trauma registry [A.R.S. § 36-2221]
- **12.** Tuberculosis control court hearing information [A.R.S. § 36-727]
- **13.** Vital Records [A.R.S. § 36-342]

c. Financial Account Data (on individuals)
- **1.** Card Holder Data (CHD) including Primary Account Number (PAN), Cardholder Name, Expiration Date, and Service Code [Payment Card Industry Data Security Standard (PCI DSS) v3.2.1]
- **2.** Credit card, charge card or debit card numbers, retirement account numbers, savings, checking or securities entitlement account numbers [A.R.S. § 44-1373]

d. Criminal Justice Information
- **1.** Child Protective Services records [A.R.S. § 41-1959]
- **2.** Criminal history record information [A.R.S. § 41-619.54]
- **3.** Criminal Justice Information [A.R.S. § 41-1750]

e. Critical Infrastructure/Fuel Facility Reports [A.R.S. § 41-4273]

f. Eligible Persons [A.R.S. § 39-123, A.R.S. § 39-124]

g. Risk Assessment and State Audit Records
- **1.** Auditor General Records [A.R.S. § 41-1279.05]
- **2.** Federal risk assessments of infrastructure [A.R.S. § 39-126]

h. Personal Identifying Information (except as determined to be public record) [A.R.S. § 18-522, 18-551]

1. Educational records [Family Educational Rights and Privacy Act (FERPA)]
2. Social Security Number [A.R.S. § 44-1373]

i. Taxpayer Information - Federal Tax Information (FTI) [A.R.S. § 42-2001] [Internal Revenue Service Publication 1075 (IRS Pub 1075)]

j. Controlled Unclassified Information (CUI) (EO 13556)

k. Licensing, Certification, Statistics and Investigation Information (of a sensitive nature)

1. Abortion reports [A.R.S. § 36-2161]
2. Child Death Records [A.R.S. § 36-3503]
3. Controlled substance records [A.R.S. § 36-2523]
4. Emergency medical service investigation records [A.R.S. § 36-2220]
5. Employment discrimination information [A.R.S. § 41-1482]
6. Health Care Cost Containment Records [A.R.S. § 36-2917]
7. Health Care Directives Registry Information [A.R.S. § 36-3295]
8. Health care entity licensing information [A.R.S. § 36-2403, A.R.S. § 36-404]
9. Medical Marijuana Records [A.R.S. § 36-2810]
10. Medical practice review [A.R.S. § 36-445, A.R.S. § 36-445.01]
11. Nursing home certification records [A.R.S. § 36-446.10]
12. Prescription information [A.R.S. § 36-2604]

l. Other State-owned Confidential Data, may include but not limited to:

1. Archaeological discoveries [A.R.S. § 39-125]
2. Attorney General opinions [A.R.S. § 38-507]
3. Tax Examination guidelines [A.R.S. § 42-2001]
4. Unclaimed property reports [A.R.S. § 44-315]
5. Vehicle information [A.R.S. § 41-3452]

m. Other Non-state-owned Confidential Data, may include, but not limited to:

1. Attorney-Client Privileged Information [A.R.S. § 41-319]
2. Bank Records [A.R.S. § 6-129]
3. Trade secrets and proprietary information [Intellectual Property laws]
4. Management and Support Information

n. Other records protected by law

6.2.2 **Public Data** - In accordance with Arizona public records law, data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

6.3 **Identification** - All data shall be identified as one of the following data classifications:

- **a.** Confidential ; or
- **b.** Public.
- **c.** Data without clear classification markings is assumed to be Confidential until otherwise determined

6.4 **Collection**

- **a.** (P) Limit Collection -
  - **1.** Encrypt confidential data
  - **2.** Properly dispose, destroy, or delete data
  - **3.** Limit access to confidential information
  - **4.** Securely store confidential data

6.5 **Handling**

6.5.1 (P) **Need to Know** - All Confidential Data shall only be given to those persons that have authorized access and a need to know the information in the performance of their duties. [**HIPAA** 164.308 (a)(3)(ii)(A) – Addressable] [**PCI DSS 7**]

6.5.2 (P) **Hand Carry** - All Confidential Data being hand-carried shall be kept with the individual and protected from unauthorized disclosure.

6.5.3 (P) **Accounting** - For bulk transfer of Confidential Data containing 500 or more records, the receipt and delivery of all Confidential Data shall be monitored and accounted for to ensure the data is not lost and potentially compromised.

6.5.4 (P) **Guardian** - When outside of controlled areas all Confidential Data shall not be left unattended, even temporarily. All Confidential Data shall remain either in a controlled environment or in the employee's physical control at all times. Mail, courier, or other mail services are considered controlled areas.

6.5.5 (P) **Out-of-sight** - All Confidential Data shall be turned over or put out of sight when visitors not authorized to view data are present.

6.5.6 (P) **Conversations** - Confidential Data shall not be discussed outside of controlled areas when visitors not authorized to hear Confidential Data are present.

6.5.7 (P) **Movement** - Unauthorized movement of Confidential Data from controlled areas shall be prohibited. [HIPAA 164.310 (d)(1)]

6.6 Transmission

6.6.1 (P) Encryption - Any external transmission of Confidential Data shall be encrypted either through link or end-to-end encryption. [HIPAA 164.308 (e)(2)(ii) – Addressable] [PCI DSS 4]

6.6.2 (P) Encryption Strength - Encryption algorithm and key length shall be compliant with current state agency minimum encryption standards as stated in the System and Communications Protection Standard [S8350].

6.7 Processing

6.7.1 (P) Approved Processing - Confidential Data shall be processed on approved devices.

6.8 Media Protection

6.8.1 (P) Confidential Data Protection - All Confidential Data shall be protected and implemented at minimum controls as stated in the ***Media Protection Policy P8250*** and ***Media Protection Standard S8250***. [HIPAA 164.310 (d)(2)] [PCI DSS 3, 9]

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 P8110 DATA CLASSIFICATION

8.2 Statewide Policy Exception Procedure

8.3 Standard S8350, System and Communications Protections

8.4 Policy P8250, Media Protection Policy

8.5 Standard S8250, Media Protection Standard

8.6 DoD 5220.22-M. National Industrial Security Program Operating Manual (NISPOM) January 1995. U.S. Government Printing Office ISBN0-16-045560-X

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

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

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

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**
12/19/23	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

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

STATEWIDE POLICY (8120): INFORMATION SECURITY PROGRAM

DOCUMENT NUMBER:	**P8120**
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 establish the information security program and responsibilities within the Budget Unit (BU).

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 - The policy shall apply to all agency information systems:

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

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

4. CONTROL SELECTION AND EXCEPTIONS

4.1 The Statewide Policies, Standards, and Procedures (PSPs) implement a control baseline for Standard and Protected state systems. By issuing the BU's own set of PSPs (based on the Statewide PSP Templates) the BU shall select a control baseline for their systems. [NIST 800-53 PL-10].

4.2 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure. This is the process of tailoring the control baseline and may be applied BU-wide or to specific BU-identified systems provided the exceptions are approved. [NIST 800-53 PL-11].

4.2.1 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.

4.2.2 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.

4.3 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.
- **b.** Ensure that by July 1 of each year all BUs have submitted the following information for approval:
  1. A state information system inventory with a system classification assignment and system owner for each state information system
  2. A system security plan and system security assessment plan for each Protected state information system
  3. A Plan of Actions and Milestones (POAM) for each Protected state information system
- **c.** Ensure that information security risks identified in Protected state information system risk assessment documentation are adequately addressed for all BUs.
- **d.** Enforce a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following mandates:
  1. Identification of a plan to address the documented risks
  2. Implementation of recommended security controls
  3. Independent security assessment on selected state information systems or controls
  4. Hosting of state system or state information system components in a state approved solution(s)
  5. Adoption of additional security requirements or procedures for the BU or selected by state systems, controls, or control environments

5.2 State Chief Information Security Officer (CISO) shall:

- **a.** Provide a format for the required compliance documents;
- **b.** 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;
- **c.** Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs;
- **d.** Identify and convey to the State CIO the risk to state information systems and data based on a review of the BU-supplied state information system inventory, system security plans, system security assessment plans and the Plan of Actions and Milestones (POAM);

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

f. Recommend a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following recommendations:
   1. Identify a plan to address the documented risks
   2. Implement recommended security controls
   3. Perform independent security assessment on selected state information systems or controls
   4. Hosting of state information system or state information system components in a state approved solution(s)
   5. Adopt any additional security requirements or procedures for the BU or selected by state systems, controls, or control environments

5.3 Enterprise Security Program Advisory Council (ESPAC)

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

b. Advise the State CISO in determination of resources needed to implement the information security programs, and availability of planned expenditures.

5.4 BU Director shall:

c. Be responsible for the correct and thorough completion of Information Security PSPs within the BU;

d. Ensure BU compliance with Information Security Program Policy; and

e. Promote efforts within the BU to establish and maintain effective use of agency information 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;

b. Ensure all BU managed systems have submitted the following documents for approval by the State CIO or designated alternate by July 1 of each year:
   1. A complete list of information systems with a system classification assignment and system owner for each agency information system
   2. A system security plan and system security assessment plan for each Protected agency information system

3. A Plan of Actions and Milestones (POAM) for each Protected agency information system

c. Ensure information security risks to Protected agency information systems, are adequately addressed according to the Protected agency information system risk assessment documentation; and

d. Be system owner for all agency information systems or delegate a system owner for BU agency information system.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU provided documentation and reports and recommend a course of action where security risks are not adequately addressed;

b. Ensure all system owners understand their responsibilities for the security planning, management, and authorization of agency information systems; and

c. Ensure the correct execution of the system security assessment plans.

5.7 System Owner shall:

a. Be responsible for the overall procurement, development, integration, modification, or operation and maintenance of the agency information system; [NIST SP 800-18]

b. Advise BU ISO as to the agency information system categorization;

c. Ensure creation of required system security plans, system security assessment plans, Plan of Actions and Milestones (POAM); and

d. Ensure the implementation of information security controls as described in system security plans and POAM.

6. STATEWIDE POLICY

6.1 System Security Planning - The BU shall implement the following controls in the planning of system security:

6.1.1 **System Security Plan** - The BU shall develop, distribute, review annually, and update an agency information system security plan. The plan shall: [NIST 800-53 PL-2]

a. Be consistent with the BU's enterprise architecture (EA);

b. Explicitly define the authorization boundary for the system including authorized connected devices (e.g., smart phones, authorized virtual office computer equipment, and defined external interfaces);

c. Describe the operational context of the agency information system in terms of missions and business processes;

d. Identify the individuals that fulfill system roles and responsibilities;

e. Identify the information types processed, stored, and transmitted by they system;

f. Provide the security categorization of the information system, including supporting rationale;

g. Describe any specific threats to the system that are of concern to the BU;

h. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

i. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

j. Provide an overview of the security and privacy requirements for the system;

k. Identify any relevant control baselines or overlays, if applicable;

l. Describe the controls in place or planned for meeting the security and privacy requirements including rationale for any tailoring decisions;

m. Include risk determinations for security and privacy architecture and design decisions;

n. Include security- and privacy-related activities affecting the system that require planning and coordination with the BU CIO, BU ISO, and system owners of affected agency information systems; and [IRS Pub 1075]

o. Be reviewed and approved by the BU CIO prior to plan implementation; and

6.1.2 (P) **Security and Privacy Architecture** – The BU shall: [NIST 800-53 PL-8][IRS Pub 1075]

a. Develop an security and privacy architecture for the agency information system that describes:
   1. The requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
   2. How the architectures are integrated into and support the enterprise architecture;
   3. Any assumptions about, and dependencies on external systems and services;

b. Annually, review and update the architectures to reflect updates in the enterprise architecture; and

c. Reflect planned architecture changes in the security and privacy plans and organizational procedures, and procurements and acquisitions.

6.2 System Security Policies – The BU shall develop security, privacy, and supply chain management risk policies and procedures to address the associated risk with the operation and use of agency information systems and the authorized processing of personally identifiable information. These policies and procedures shall include the following:

a. Data Classification Policy and Procedures (P8110)

b. Information Security Program Policy and Procedures, including security, privacy, and supply chain risk management (P8120)
[NIST 800-53 CA-1] [NIST 800-53 PL-1] [NIST 800-53 PM-1] [NIST 800-53 RA-1][SR-1]

c. System Security Acquisition Policy and Procedures (P8130)
[NIST 800-53 SA-1]

d. Security Awareness Training Policy and Procedures (P8210)
[NIST 800-53 AT-1]

System Security Maintenance Policy and Procedures (P8220)
[NIST 800-53 CM-1] NIST 800-53 MA-1] [NIST 800-53 SI-1]

e. Contingency Planning Policy and Procedures (P8230) [NIST 800-53 CP-1]

f. Incident Response Planning Policy and Procedures (P8240);
[NIST 800-53 IR-1]

g. Media Protection Policy and Procedures (P8250) [NIST 800-53 MP-1]

h. Physical Security Protection Policy and Procedures (P8260)
[NIST 800-53 PE-1]

i. Personnel Security Policy and Procedures (P8270) [NIST 800-53 PS-1]

j. Acceptable Use Policy, including social media, networking restrictions, restrictions on posting on public websites, and use of organizational identifiers (P8280) [NIST 800 53 AC-1] [NIST SP 800 53 PL-4a, PL-4(1)]

k. Account Management Policy and Procedures (P8310)

l. Access Controls Policy and Procedures (P8320) [NIST 800-53 AC-1] [HIPAA 164.310 (a)(2)(ii)]

m. System Security Audit Policy and Procedures (P8330) [NIST 800-53 AU-1]

n. Identification and Authentication Policy and Procedures (P8340)
[NIST 800-53 IA-1]

o. System and Communication Protections Policy and Procedures (P8350) [NIST 800-53 SC-1]

p. System Privacy Policy and Procedures (P8410)

q. System Privacy Notice (S8410)

6.2.1 **Policy Development, Maintenance, and Distribution** – The BU shall: [HIPAA 164.316 (a), (b)(1), (b)(2)] [PCI DSS 12.1.1]

a. Designate an agency official to develop, document and disseminate , to appropriate personnel and roles, the policies and procedures for each agency information system.

b. Maintain the organizational security policies and procedures;

c. These policies shall be consistent with applicable laws, directives, regulations, policies, standards, and guidelines.

d. Retain these documents for six years from the date of its creation or the date it last was in effect, whichever is later. 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;

e. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

f. Review documentation at least annually, and update as needed, in response to environmental or operational changes affecting the security of the Confidential information.

6.3 Risk Management - To appropriately manage security risk to agency information systems, the following activities shall be performed for each agency information system: [HIPAA 164.308 (a)(1)(i), (a)(1)(ii)(B)]

6.3.1 **Impact Assessment** - A potential impact assessment shall be performed for each agency information system to determine the system categorization. An impact assessment considers the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the agency information system and/or its data. Impact assessments result in the determination of impact based on the following definitions:

a. Limited Adverse Impact - The loss of confidentiality, integrity, or availability could be expected to have limited adverse effect on

organizational operations, organizational assets or individuals. For example, it may:

1. Cause a degradation in mission capability, to an extent and duration, that the organization is able to perform its primary function, but the effectiveness of the function is noticeably reduced;
2. Result in minor damage to organizational assets;
3. Result in a minor financial loss; or
4. Result in minor harm to individuals.

b. Serious Adverse Impact - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals. For example, it may:

1. Cause a significant degradation in mission capability, to an extent and duration, that the organization is able to perform it primary function, but the effectiveness of the function is significantly reduced;
2. Result in significant damage to organizational assets;
3. Result in a significant financial loss; or
4. Result in significant harm to individuals that do not involve loss of life or serious life threatening injuries.

NOTE: Impact assessment on agency information systems storing, processing, or transmitting Confidential Data may result in a serious adverse impact.

6.3.2 **System Categorization** – The BU shall categorize agency information systems and the information it processes, stores, and transmits, document the security categorization results (including supporting rationale) in the security plan for the agency information system; and verify that the security categorization decision is reviewed by the BU CSO and approved by the BU CIO. All agency information systems are categorized according to the potential impact to the state or citizens resulting from the disclosure, modification, destruction, or non-availability of system functions or data. [NIST 800-53 RA-2]

6.3.3 **System Categorization Levels** - The following system categorization levels shall be applied to all agency information systems:

a. Standard - Loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact on the BU's operations, organizational assets, or individuals, including citizens

b. Protected - Loss of confidentiality, integrity, or availability could be expected to have serious, severe, or catastrophic adverse impact on organizational, assets, or individuals, including citizens

6.3.4 **Risk Assessment** - The BU shall: [NIST 800-53 RA-3]
[HIPAA 164.308 (a)(1)(ii)(A)]

a. Conduct an assessment of security and privacy risk, including identification of threats to and vulnerabilities in the system, the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the agency information system, the information it processes, stores, or transmits, and any related information;

1. Determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
2. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
3. Perform and document the risk assessment annually or whenever there are significant changes to the information system or environment of operations (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. [PCI DSS 12.2] ;
4. Review risk assessment results annually;
5. Disseminate risk assessment results to the BU CIO, BU ISO, agency information system owner, and other BU-defined personnel or roles; and

b. Conduct an assessment of supply chain risks associated with BU systems, system components, and system services. The supply chain risk assessment shall be updated annually, when there are significant changes to the supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. [NIST 800-53 RA-3(1)].

6.3.5 **Vendor Risk Management** – The BU shall protect against vendor (e.g., Cloud Service Providers, contractors, supply chain) threats to the information system, system component, or information service by employing a vendor risk management program as part of a comprehensive, defense in-breadth information security strategy. [NIST 800-53 SA-12][SR-1]

6.3.6 **(P) Third Party Risk Assessment –** The BU shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, modification, or destruction of third parties authorized by the BU to process, store, or transmit Confidential Data. [HIPAA 164.308 (a)(ii)(A)]

6.3.7 **Vulnerability Scanning** – The BU shall establish a process to identify security vulnerabilities implementing the following: [NIST 800-53 RA-5] [PCI DSS 6.1, 11.2]

a. use reputable outside sources for security vulnerability information, [PCI DSS 6.1]

b. assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities [PCI DSS 6.1]

c. Monitor and can for vulnerabilities in the agency information system and hosted applications quarterly and when new vulnerabilities potentially affecting the system/applications are identified and reported from internal and external interfaces; [PCI DSS 11.2.3]

d. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact.

e. Analyze vulnerability scan reports and results from vulnerability monitoring;

f. Remediate legitimate vulnerabilities within 30 days in accordance with an organization assessment of risk;

g. Share information obtained from the vulnerability monitoring process and control assessments with BU-defined personnel or roles to help eliminate similar vulnerabilities in other agency information systems (i.e. systemic weaknesses or deficiencies.);

h. Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components; [NIST 800-53 RA-5(11)];

i. (P) Establish a process to identify and assign risk ranking to newly discovered security vulnerabilities; [PCI DSS 11.2]

j. (P) Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved according to vulnerability ranking. [PCI DSS 11.2.1]

   1. (P) Update tool capability - The BU shall employ vulnerability scanning tools that include the capability to readily update the agency information system vulnerabilities to be scanned; [NIST 800-53 RA-5] [IRS Pub 1075]

   2. (P) Update prior to new scans - The BU shall update the agency information system vulnerabilities scanned prior to new scans; [NIST 800-53 RA-5(2)] [IRS Pub 1075]

3. (P) Provide privileged access - The agency information system implements privileged access authorization to BU-defined components containing highly Confidential Data (e.g., databases); and [NIST 800-53 RA-5(5)]
[IRS Pub 1075]

4. (P) Qualify scanning vendors - The BU shall employ an impartial and qualified scanning vendor to conduct quarterly external vulnerability scanning. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment and is qualified in the use and interpretation of vulnerability scanning software and techniques. [PCI DSS 11.2.2]

6.4 Information Security Program Management - The BU shall implement the following controls in the management of the information security program:

6.4.1 **Senior Information Security Officer** - The BU shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a BU-wide information security program. [NIST 800-53 PM-2] [EO 2008-10]

6.4.2 **Information Security Resources** - The BU shall include the resources needed to implement the information security program and document all exceptions to this requirement. This includes employing a business case to record the resources required, and ensuring that information security resources are available for expenditure as planned.

6.4.3 **Plan of Action and Milestones Process** - The BU shall: [NIST 800-53 PM-4]

a. Implement a process for ensuring that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated agency information systems are:
  1. Developed and maintained
  2. Reported in accordance with reporting requirements
  3. Documented with the remedial information security, privacy, and supply chain management actions to adequately respond to risk to organizational operations, assets, individuals, other organizations, and the state

b. Review plans of action and milestones for consistency with the organizational risk management strategy and BU-wide priorities for risk response actions.

6.4.4 **System Inventory** - The BU shall develop and annually update an inventory of its information systems, including a classification of all system components (e.g., Standard or Protected). [NIST 800-53 PM-5]

6.4.5 **Measures of Performance** - The BU shall develop, monitor, and report on the results of information security and privacy measures of performance. [NIST 800-53 PM-6]

6.4.6 **Enterprise Architecture** - The BU shall develop and maintain an enterprise architecture with consideration for information security, privacy, and resulting risk to organizational operations, organizational assets, individuals, other organizations, and the agency. [NIST 800-53 PM-7]

6.4.7 **Critical Infrastructure Plan –** If applicable, the BU shall address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. [NIST 800-53 PM-8]

6.4.8 **Risk Management Strategy** - The BU shall:

- **a.** Develop a comprehensive strategy to manage security risk to organizational operations and assets, individuals, other organizations, and the agency associated with the operation and use of agency information systems; privacy risk to individuals resulting from the authorized processing of personally identifiable information;
- **b.** Implement this strategy consistently across the organization; and
- **c.** Review and update the risk management strategy annually or as required to address organizational changes.[NIST 800-53 PM-9]

6.4.9 **Supply Chain Risk Management Strategy** - The BU shall: [NIST 800-53 SR-2]

- **a.** Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems, system components, or system services;
- **b.** Review and update the supply chain risk management plan annually or as required to address threat, organizational, or environmental changes;
- **c.** Protect the supply chain risk management plan from unauthorized disclosure and modification;
- **d.** Establish a supply chain risk management team to lead and support the supply chain risk management activities. [NIST 800-53 SR-2(1)]
- **e.** Implement supply chain risk management controls and processes, including: [NIST 800-53 SR-3]

1. Establishing a process(es) to identify and address weaknesses or deficiencies in the key supply chain elements and processes in coordination with supply chain personnel;
2. Employing adequate controls to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related event; and
3. Documenting the selected and implemented supply chain processes and controls in the supply chain risk management plan;

f. Employ appropriate acquisition strategies, contract tool, and procurement methods to protect against, identify, and mitigate supply chain risks; [NIST 800-53 SR-5];

g. Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide; [NIST 800-53 SR-6];

h. Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessments or audits; [NIST 800-53 SR-8];

i. Inspect the appropriate systems or system components randomly but at sufficient frequency to adequately detect tampering [NIST 800-53 SR-10];

j. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and report counterfeit system components to the source of the counterfeit component and the State CISO. The BU shall: [NIST 800-53 SR-11]

1. Train appropriate personnel to detect counterfeit system components (including hardware, software, and firmware); [NIST 800-53 SR-11(1)]
2. Maintain configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service. [NIST 800-53 SR-11(2)]

k. Dispose of system components using the approved techniques and methods that ensure the sanitization of sensitive data. [NIST 800-53 SR-12]

6.4.10 **Risk Response** - The BU shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with BU-defined risk tolerance. [NIST 800-53 RA-7]

6.4.11 **Privacy Impact Assessments** - The BU shall conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that processes personally identifiable information and before initiating a new collections of personally identifiable information that will be processed using information technology and includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than BUs or state employees. [NIST 800-53 RA-8]

6.4.12 **Criticality Analysis** - The BU shall identify critical system components and functions by performing a criticality analysis for BU systems, system components, and system services when the system is being designed, modified, or upgraded. [NIST 800-53 RA-9]

6.4.13 **Security Authorization Process** – The BU shall: [NIST 800-53 PM-10]

- **a.** Manage the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
- **b.** Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
- **c.** Fully integrates the security authorization processes into an BU-wide risk management program.

6.4.14 **Mission/Business Process Definition** - The BU shall: [NIST 800-53 PM-11]

- **a.** Define mission/business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the agency; and
- **b.** Determine information protection needs and personally identifiable information processing needs arising from the defined mission/business processes; and
- **c.** Revise the process as necessary, until achievable protection needs are obtained.

6.4.15 **Insider Threat Program** - The BU shall implement an insider threat program that includes a cross-discipline insider threat incident handling team. [NIST 800-53 PM-12]

6.4.16 **Information Security Workforce** – The BU shall establish an information security and privacy workforce development and improvement program. [NIST 800-53 PM-13]

6.4.17 **Testing, Training, and Monitoring** - The BU shall: [NIST 800-53 PM-14]

a. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained; and continue to be executed in a timely manner; and

b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and BU-wide priorities for risk response actions.

6.4.18 **Contacts with Security Groups and Associations** - The BU shall establish and institutionalize contact with selected groups and associations within the security community to: [NIST 800-53 PM-15]

a. Facilitate ongoing security education and training for BU personnel;

b. Maintain currency with recommended security practices, techniques, and technologies; and

c. Share current security-related information including threats, vulnerabilities, and incidents.

6.5 Control Assessments and Authorizations - The BU shall implement the following controls in the assessment and authorization of agency information systems:

6.5.1 **Control Assessments –** The BU shall: [NIST 800-53 CA-2] [HIPAA 164.308 (a)(8)]

a. Develop a control (e.g., security and privacy controls) assessment plan that describes the scope of the assessment including security controls under assessment, assessment procedures to be used to determine security control effectiveness, and assessment environment, assessment team, and assessment roles and responsibilities;

b. Assess the controls in the information system and its environment of operation periodically to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. Produce a control assessment report that documents the results of the assessment; and

d. Provide the results of the control assessment to the BU CIO, BU CSO, BU Privacy Officer, State Privacy Officer, and the State CSO.

6.5.2 **(P) Independent Assessors** - The BU shall employ impartial assessors or assessment teams to conduct control assessments. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment. [NIST 800-53 CA-2(1)] [IRS Pub 1075]

6.5.3 **(P) Third Party Security Assessment** - The BU shall conduct a security assessment with third parties authorized by the BU that process, store, or transmit Confidential Data. [HIPAA 164.308 (a)(8)]

6.5.4 **(P) Wireless AP Testing** - The BU shall test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. [PCI DSS 11.1]

6.5.5 **System Interconnections** – The BU shall: [NIST 800-53 CA-3]

a. Authorize connections from the agency information system to other information systems through the use of interconnection security agreements; information exchange agreements; memorandum of understanding or agreement; service level agreement; user agreements; or nondisclosure agreements

b. Document, for each interconnection, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update agreements annually:

1. (P) Restrictions on External System Connections - The BU shall employ a “deny-all, permit-by-exception” policy for allowing Protected agency information systems to connect to external information systems at managed interfaces. [NIST 800-53 SC-7(5)] [IRS Pub 1075]

2. (P) Third Party Authorization – The BU shall permit a third party, authorized by the BU to process, store, or transmit Confidential data, to create, receive, maintain, or transmit Confidential information on the BU’s behalf only if covered entity obtains satisfactory assurances that the third party will appropriately safeguard the information. The BU documents the satisfactory assurance through a written contract or other arrangement with the third party. [HIPAA 164.308 (b)(1) and (b)(2)]

6.5.6 **Plan of Action and Milestones** - The BU shall: [NIST 800-53 CA-5]

a. Develop a plan of action and milestones for the agency information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

6.5.7 **Security Authorization** – The BU shall: [NIST 800-53 CA-6]

- **a.** Assign a senior official the authorizing official for the information system and accepting common controls inherited by Statewide or other organizational systems;
- **b.** Ensure the authorizing official authorizes the agency information system for processing and accepts the inherited common controls before commencing operations; and
- **c.** Update the security authorization every three years.

6.5.8 **Continuous Monitoring** - The BU shall develop a system-level continuous monitoring strategy and implements a BU-level or continuous monitoring program that

- **a.** includes: [NIST 800-53 CA-7] [HIPAA 164.308 (a)(1)(ii)(D)]
  1. Establishment of system-level metrics to be monitored;
  2. Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;
  3. Ongoing security control assessments in accordance with the BU continuous monitoring strategy;
  4. Ongoing security status monitoring of the BU-defined system-level metrics in accordance with the BU continuous monitoring strategy;
  5. Correlation and analysis of security-related information generated by assessments and monitoring;
  6. Response actions to address results of the analysis of security-related information; and
  7. Reporting the security status of the BU and the information system to the State CISO quarterly;
- **b.** Employs independent assessors or assessment teams to monitor the controls in the system on an ongoing basis; [NIST 800-53 CA-7(1)]; and
- **c.** Ensures risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness, compliance, and change monitoring. [NIST 800-53 CM-7(4)].

6.5.9 (P) **Penetration Testing** - The BU shall conduct penetration testing annually and after significant infrastructure or application upgrade or modification on Protected agency information systems from internal and external interfaces. These penetration tests must include network-layer penetration tests, segmentation

control tests, and application-layer penetration tests. [NIST 800-53 CA-8] [PCI DSS 11.3, 11.3.1, 11.3.2]

- **a.** (P) Independent Penetration Agent or Team - The BU shall employ an impartial penetration agent or penetration team to perform penetration testing. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment. [NIST 800-53 CA-8]
- **b.** (P) Segmentation Testing – The BU shall ensure that penetration testing includes verification of segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all Protected systems and components systems from non-protected systems and components. [PCI DSS 11.3.4]
- **c.** (P) Address Penetration Testing Issues – The BU shall ensure that exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. [PCI DSS 11.3.3]

6.5.10 **Internal System Connections** - The BU shall authorize internal connections of other agency information systems or classes of components (e.g., digital printers, laptop computers, mobile devices, facsimile machines, sensors, and servers) to the agency information system and, for each internal connection, shall document the interface characteristics, security and privacy requirements and the nature of the information communicated. The BU shall terminate internal system connections after the need for such connections is no longer required and shall review these connections annually. [NIST 800-53 CA-9] [IRS Pub 1075]

6.6 Establish Operational Procedures – The (Agency) BU shall ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. [PCI DSS 11.6]

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 P8120 Information Security Program

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 Executive Order 2008-10

8.8 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number GS 1005, Arizona State Library, Archives and Public Records, Item Number 16

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**
12/19/23	**Annual Updates**	**4.0**	

			Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer

	STATEWIDE # POLICY	**State of Arizona**

STATEWIDE POLICY (8130): SYSTEM SECURITY ACQUISITION AND DEVELOPMENT

DOCUMENT NUMBER:	**P8130**
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 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 vulnerability. 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, 6.4.5]

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; and [PCI DSS 6.4.3]

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]

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;

4. 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]

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

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

b. 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;

c. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

d. 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)]

6.6.1 **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]

6.6.2 **(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]

6.7 (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.

6.8 (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.

6.8.1 (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.

6.8.2 (P) **Threat and Vulnerability Analyses** - The BU shall require the developer of the system, system component, orsystem service to perform threat modeling and vulnerabilities analyses 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.

6.8.3 (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.

6.8.4 (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]

6.9 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**
5/26/21	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer**
12/19/23	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

	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**
5/19/2023	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

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

STATEWIDE POLICY (8220): SYSTEM SECURITY MAINTENANCE

DOCUMENT NUMBER:	**P8220**
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 technology (IT) 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 the baseline controls for management and maintenance of agency system controls.

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 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 subject matter experts 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 The 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 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 State CIO 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 BU Director shall:

- **a.** Be responsible for the correct and thorough completion of Agency Information Security PSPs within the BU;
- **b.** Ensure BU compliance with System Security Maintenance Policy; and
- **c.** 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 System Security Maintenance Policy is 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 agency information security PSPs;
- **b.** Ensure the development and implementation of an adequate controls enforcing the System Security Maintenance Policy for the BU agency systems; and
- **c.** Ensure all personnel understand their responsibilities with respect to secure system management and maintenance.

6. STATEWIDE POLICY

6.1 System Configuration Management

6.1.1 Configuration Management Plan - The BU shall develop, document, and implement a configuration management plan for agency systems that will:

- **a.** Address the roles, responsibilities, and configuration management processes and procedures;
- **b.** Establish a process for identifying configuration items throughout the system development lifecycle and for managing the configuration of the configuration items;
- **c.** Define the configuration items for the agency system and place the configuration items under configuration management;

d. Ensure configuration items are reviewed and approved by BU-identified roles; and

e. Protect the configuration management plan from unauthorized disclosure and modification. [National Institute of Standards and Technology (NIST) 800 53 CM-9]

6.1.2 Baseline Configuration - The BU shall develop, document, and maintain a current baseline configuration of each agency system. [NIST 800 53 CM-2]

a. Baseline Configuration Reviews and Updates - The BU shall review and update the baseline configurations for systems, at least annually, upon significant changes to system functions or architecture, and as an integral part of system installations and upgrades. [NIST 800-53 CM-2] [Internal Revenue Service (IRS) Pub 1075]

1. (P) Automated Support for Accuracy and Currency - The BU shall maintain currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms, tools, or services. [NIST 800-53 CM-2(2)]

b. (P) **Baseline Configuration Retention** - The BU shall retain at least one previous version of baseline configurations to support rollback. [NIST 800 53 CM-2 (3)] [IRS Pub 1075] 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: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 8.

c. (P) **Baseline Configuration for External High Risk Areas** - The BU shall establish separate baseline configurations for computing resources (e.g., notebook computers) issued to individuals traveling to locations deemed to be a significant risk. The organization shall apply BU-identified protective controls (e.g., examination for physical tampering, purge and reimage disk drives) to these devices when the individuals return from travel. [NIST 800-53 CM-2 (7)] [IRS Pub 1075]

6.1.3 (P) **Configuration Change Control** - The BU shall: [NIST 800 53 CM-3] [IRS Pub 1075]

a. Determine the types of changes to the agency system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the agency system and approves or disapproves such changes with explicit consideration for security impact analysis;

c. Document configuration change decisions associated with the agency system;

d. Implement approved configuration-controlled changes to the system;

e. Retain activities associated with configuration-controlled changes to the agency system in compliance with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 8;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration control activities through an established configuration control board that convenes at least monthly to review the activities associated with configuration-controlled changes to agency systems.

6.1.4 Change Approval - The BU shall review and approve/disapprove proposed configuration-controlled changes to the agency systems. Security and privacy impact analysis shall be included as an element of the decision. [NIST 800 53 CM-4]

a. (P) **Test, Validate, and Document Changes** - Approved changes shall only be implemented on an operational system after the change control board ensures that the change has been tested, validated, and documented. [NIST 800 53 CM-3 (2)] [IRS Pub 1075]

b. (P) Verification of Controls - After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regards to meeting the security and privacy requirements for the system. [NIST 800-53 CM-4(2)]

c. (P) **Security and Privacy Representatives** - Require that the change control board have representatives of security and privacy. [NIST 800-53 CM-3(4)]

6.1.5 (P) **Change Restriction Enforcement** - The BU shall ensure that adequate physical and/or logical controls are in place to enforce restrictions associated with changes to agency systems. The BU shall permit only qualified and authorized individuals to access agency systems for the purpose of initiating changes, including upgrades and modifications. [NIST 800 53 CM-5] [IRS Pub 1075]

6.1.6 Configuration Settings - The BU shall: [NIST 800 53 CM-6]

a. Establish and document configuration settings for components employed within the agency system using Statewide, BU-wide, or agency information specific security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

b. Implement the configuration settings;

c. Identify documents, and approve any deviations from established configuration settings for all system components for which security checklists have been developed and approved; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

6.1.7 Agency system Component Inventory - The BU shall develop and document an inventory of agency system components (including authorized wireless access points and business justification for those access points) that accurately reflects the system, is consistent with the defined boundaries of the agency system, is at the level of granularity deemed necessary for tracking and reporting hardware and software, and includes hardware inventory specifications (e.g., manufacturer, device type, model, serial number, and physical location), software license information, software version numbers, component owners, and for networked components: machine names and network addresses. The inventory shall not duplicate an accounting of components assigned to any other system. [NIST 800 53 CM-8] [PCI DSS 2.4 , 11.1.1]

a. Inventory Reviews and Updates - The BU shall review and update the system component inventory annually and as an integral part of component installations, removals, and system updates. [NIST 800 52 CM-8 (1)]

b. (P) Inventory Automated Detection - The BU shall detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms quarterly, and take actions to disable network access, isolate the component, or notify the appropriate BU personnel of the unauthorized component when unauthorized components are detected. [NIST 800 53 CM-8 (3)] [IRS Pub 1075]

c. (P-PCI) Inventory Payment Card Data Capture Devices - The BU shall maintain an up-to-date list of devices. The list shall include device make and model, device location, and device serial number (or other method of unique identification). [PCI DSS 9.9, 9.9.1]

6.1.8 (P) **Confidential Information Location** - The BU shall identify and document the location of Confidential data and specific components on which the information is processed and stored; identify and document the users who have access to the system and system components where the information is processed and stored; and document changes to the location where the information is processed and stored. [NIST 800-53 CM-12]

a. (P) Automated Tools to Support Confidential Information Location - The Bu shall use automated tools to identify COnfidential information on systems and system components to ensure controls are in place to protect BU Confidential information and individual privacy. [NIST 800-53 CM-12(1)]

6.1.9 Software Usage Restrictions - The BU shall use software and associated documentation in accordance with contract agreements and copyright laws; track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. [NIST 800 53 CM-10]

6.2 Agency system Maintenance - In addition to the change management requirements of Section 6.1, the following requirements apply to the maintenance of agency systems:

6.2.1 Controlled Maintenance - The BU shall: [NIST 800 53 MA-2]

b. Schedule, document, and review records of maintenance, repair, and replacement on agency system components in accordance with manufacturer or vendor specifications and BU requirements;

c. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced onsite or removed to another location;

d. Explicitly approve the removal of the agency system or system components from the BU facilities for off site maintenance, repair, or replacement;

e. Sanitize equipment to remove Confidential information from associated media prior to removal from BU facilities for off site maintenance, repair, or replacement;

f. Ensure equipment removed from the BU facilities is properly sanitized prior to removal. (Refer to Media Protection Policy P8250 for appropriate sanitization requirements and methods); and

g. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance,repair, or replacement actions. These checks are documented in BU maintenance records and shall include date and time of maintenance, a description of the maintenance performed, names of individuals or groups performing the maintenance, the name of the escort (if applicable), and system components or equipment removed or replaced.

6.2.2 (P) **Maintenance Tools** - The BU shall approve, control, and monitor the use of system maintenance tools and shall review previously approved system maintenance tools annually. [NIST 800 53 MA-3] [IRS Pub 1075]

a. (P) Tool Inspection - Maintenance tools, and/or diagnostic and test programs used by maintenance personnel shall be inspected for improper

or unauthorized modifications including malicious code prior to the media being used in the agency system. [NIST 800 53 MA-3(1)(2)] [IRS Pub 1075]

b. (P) Prevent Unauthorized Removal - The BU shall prevent the removal of maintenance equipment containing Confidential information by verifying that there is no Confidential information contained on the equipment; sanitizing or destroying the equipment; retaining the equipment within the BU facility; or obtaining an exemption from the BU ISO explicitly authorizing removal of the equipment from the BU facility. [NIST 800-53 MA-3(3)]

6.2.3 Remote Maintenance - The BU shall: [NIST 800 53 MA-4]

a. Approve and monitor remote maintenance and diagnostic activities;

b. Allow the use of remote maintenance and ensure diagnostic tools are consistent with BU policy and documented in the security plan for the agency system;

c. Employ two-factor authentication for the establishment of remote maintenance and diagnostic sessions;

d. Maintain records for all remote maintenance and diagnostic activities in compliance with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 3; and

e. Terminate network sessions and connections upon the completion of remote maintenance and diagnostic activities.

6.2.4 Maintenance Personnel - The BU shall: [NIST 800 53 MA-5]

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Ensure non-escorted personnel performing maintenance on agency systems have required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

6.2.5 (P) **TImely Maintenance** - The BU shall obtain maintenance support and/or spare parts for critical systems and system components within BU-defined time periods of failure. [NIST 800-53 MA-6]

6.3 System and Information Integrity [HIPAA 164.132(c),(1)]

6.3.1 Flaw Remediation - The BU shall: [NIST 800 53 SI-2]

- **a.** Identify, report, and correct system flaws;
- **b.** Test software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects prior to installation;
- **c.** Install security-relevant software and firmware updates and patches within 30 days of release from the vendor; and [PCI DSS 6.2]
- **d.** Incorporate flaw remediation into the organizational configuration management process.

6.3.2 (P) **Automated Flaw Remediation System** - The BU shall employ an automated mechanism monthly to determine if system components have applicable security-relevant software and firmware updates installed. [NIST 800 53 SI-2(2)] [IRS Pub 1075]

6.3.3 Malicious Code Protection - The BU shall: [NIST 800 53 SI-3] [HIPAA 164.308(a)(5)(ii)(B) - Addressable] [PCI DSS 5.1]

- **a.** Implements a centrally managed malicious code protection mechanisms at agency system entry and exit points and all systems commonly affected by malicious software particularly personal computers and servers to detect and eradicate malicious code; [NIST 800 53 SI-3, PL-9] [PCI DSS 5.1, 5.1.1]
- **b.** For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. [PCI DSS 5.1.2]
- **c.** Update malicious code protection mechanisms automatically whenever new releases are available in accordance with the BU's configuration management policy and procedures; [NIST 800 53 SI-3)]
- **d.** Configure malicious code protection mechanisms to:
  - Perform periodic scan of the agency system weekly and real-time scans of files from external sources at the endpoint, and network entry and exit points as the files are downloaded, opened, or executed; [PCI DSS 5.2]
  - Block and quarantine malicious code and/or send an alert to a system administrator in response to malicious code detection; and
  - Generate audit logs. [PCI DSS 5.2]
- **e.** Address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of the agency system; and
- **f.** Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period. [PCI DSS 5.3]

6.3.4 system Monitoring - The BU shall: [NIST 800 53 SI-4a] [HIPAA 164.308(a)(1)(iii)(D)] [PCI DSS 11.4]

a. Monitor the agency systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections;

b. Identify unauthorized use of the agency system through BU-defined intrusion-monitoring tools;

c. Invoke internal monitoring capabilities or deploy monitoring devices strategically within the agency system, including at the perimeter and critical points inside the environment to collect essential security-relevant information and to track specific types of transactions of interest to the BU; [PCI DSS 11.4]

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the agency based on Confidential information;

f. Receive alerts from:

- malicious code protection mechanisms;
- intrusion detection or prevention systems;
- boundary protection mechanisms such as firewalls, gateways, and routers;

g. Obtain legal opinion with regard to system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations; and

h. Provide state-defined system monitoring data to the state-defined roles on a state-defined basis.

i. (P) Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security and privacy implications. [NIST 800-53 SI-4(12)]

j. (P) Implement host-based monitoring mechanism on systems that receive, process, store, or transmit Confidential information.[NIST 800-53 SI-4(23)]

6.3.4.1. Updates - All intrusion detection systems and/or prevention engines, baselines, and signatures shall be kept up-to-date. [PCI DSS 11.4]

6.3.4.2. (P) Automated Tools - The BU shall employ automated tools and mechanisms to support near real-time analysis of events. [NIST 800-53 SI-4(2)] [IRS Pub 1075]

6.3.4.3. (P) Inbound and Outbound CommunicationsTraffic - The BU shall determine criteria for unusual or unauthorized activities or conditions

for inbound and outbound communications traffic, monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. [NIST 800 53 SI-4(4)] [IRS Pub 1075]

6.3.4.4. (P) System Generated Alerts - The BU shall ensure the system alerts system administrators when the BU-defined indicators of compromise or potential compromise occur. [NIST 800 53 SI-4(5)] [IRS Pub 1075] [PCI DSS 11.4]

6.3.5 Security Alerts, Advisories, and Directives - The BU shall implement a security alert, advisory and directive program to: [NIST 800 53 SI-5]

- **a.** Receive information security alerts, advisories, and directives from the agency and additional services as determined necessary by the BU ISO on an on-going basis;
- **b.** Generate internal security alerts, advisories, and directives as deemed necessary;
- **c.** Disseminate security alerts, advisories, and directives to appropriate employees and contractors, other organizations, business partners, supply chain partners, external service providers, and other supporting organizations as deemed necessary; and
- **d.** Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

6.3.6 (P) **Integrity Verification Tools** - The BU shall employ integrity verification tools to detect unauthorized changes to critical software, system files, configuration files, or content files. Upon detection of such changes the BU shall perform BU-defined actions. [NIST 800 53 SI-7] [IRS Pub 1075] [HIPAA 164.312(c)(1)] [PCI DSS 11.5]

6.3.6.1 (P) **Integrity Checks** - The BU shall ensure agency systems will perform integrity checks at least weekly and at start up, the identification of a new threat to which agency systems are susceptible, and the installation of new hardware, software, or firmware. [NIST 800-53 SI-7(1)] [IRS Pub 1075] [PCI DSS 11.5]

6.3.6.2 (P) **Automated Notifications of Integrity Violations** - The BU shall employ automated tools that provide notification to BU-defined personnel or roles upon discovering discrepancies during integrity verification. [NIST 800-53 SI-7(2)]

6.3.6.3 (P) **Incident Response Integration** - The BU shall incorporate the detection of unauthorized changes to critical system files into the BU incident response capability. [NIST 800-53 SI-7(7)] [IRS Pub 1075]

6.3.7 Spam Protection - The BU shall employ spam protection mechanisms at agency system entry and exit points to detect and take action on unsolicited messages and updates spam protection mechanisms automatically updated when new releases are available. [NIST 800-53 SI-8, 8(2)] [IRS Pub 1075]

a. **Central Management** - Spam protection mechanisms are centrally managed. [NIST 800-53 PL-9] [IRS Pub 1075]

b. Automated Updates - Spam protection mechanisms automatically update daily. [NIST 800-53 SI-8(2)]

c. Continuous Learning Capability - Spam protection mechanisms incorporate a learning capability to more effectively identify legitimate communications traffic. [NIST 800-53 SI-8(3)].

6.3.8 (P) **Information Input Validation** - The BU shall ensure agency systems check the validity of system inputs from untrusted sources, such as user input. [NIST 800-53 SI-10] [IRS Pub 1075]

6.3.9 **Error Handling** - The BU shall ensure the agency system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries and reveals error messages only to system administrator roles. [NIST 800-53 SI-11] [IRS Pub 1075]

6.3.10 **Information Management and Retention** - The BU shall handle and retain information within the agency system and information output from the system in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [NIST 800-53 SI-12] [ARS 44-7041] [Arizona State Library Retention Schedules for Information Technology (IT) Records]

a. (P) The BU shall limit personally identifiable information being processed in the information life cycle to BU-defined elements of personally identifiable information. [NIST 800-53 S-12(1)]

b. (P) The BU shall use BU-defined techniques to minimize the use of personally identifiable information for research, testing, or training. [NIST 800-53 SI-12(2)]

c. The BU shall use the techniques consistent with those defined in the Media Protection Policy (P8250) and to dispose of, destroy, or erase information following the retention period in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [NIST 800-53 SI-12(3)] Arizona State Library Retention Schedules for Information Technology (IT) Records]

6.3.11 (P) **Memory Protection** - The BU shall ensure the system implements controls to protect the system memory from unauthorized code execution. [NIST 800-53 SI-16].

6.3.12 **Establish Operational Procedures** – The BU shall ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all **affected** parties. [PCI DSS 5.4]

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 8220 System Security Maintenance

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK P8250 Media Protection

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

8.5 ARS 44-7041

8.6 Arizona State Library Retention Schedules for Information Technology (IT) Records

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

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

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

8.10 General Records Retention Schedule for All Public Bodies, Information Technology (IT) Records, Schedule Number: 000-12-41, Arizona State Library, Archives and Public Records, Item Numbers 3 and 8

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**
5/19/2023	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**

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

STATEWIDE POLICY (8230): CONTINGENCY PLANNING

DOCUMENT NUMBER:	**P8230**
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.)§ 18-104 and § 18-105.

2. PURPOSE

The purpose of this policy is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability. [NIST 800-34]

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.** 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 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 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 BU Director shall:

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

c. Identify and convey contingency planning needs;

d. Ensure compliance with BU PSPs; and

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

5.5 The BU CIO shall:

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

b. Assign the necessary resources to document, implement, and maintain the contingency plan, including the following roles:

c. Recommend/Ensure continuity plans are documented in the contingency plan;

d. Approve developed and modified contingency plan; and

e. Ensure Contingency Planning Policy is 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 Information Security PSPs;

b. Ensure the development and implementation of adequate controls enforcing the Contingency Planning Policy for the BU;

c. Ensure all personnel understand their responsibilities with respect to business continuity and disaster recovery planning; and

d. Work with project leader on security and privacy related issues involving the development, maintenance, or testing of the contingency plan.

5.7 System owners shall:

a. Participate in establishing, approving, and maintaining policies for the protection controls applicable to the agency systems under their control; and

b. Work with the project leader on agency system related issues involving the development, maintenance, or testing of the contingency plan.

5.8 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on the Contingency Planning Policy; and

b. Monitor employee activities to ensure compliance.

5.9 System Users of agency systems shall:

- **a.** Become familiar with this policy and related PSPs; and
- **b.** Adhere to PSPs regarding the Contingency Planning Policy.

6. STATEWIDE POLICY

6.1 Develop Contingency Plan – The BU shall develop a contingency plan that: [National Institute of Standards and Technology (NIST) 800-53 CP-2] [Health Insurance Portability and Protection Act (HIPAA) 164.308(a)(7)(i), 164.308(a)(7)(ii)(b), 164.308(a)(7)(ii)(c), 164.310(a)(2)(i)]

- **a.** Identifies essential mission and business functions and the associated contingency requirements consistent with *Establishing an Essential Records List* published by Arizona State Library, Archives and Public Records;
- **b.** Provides recovery objectives, restoration priorities, and metrics;
- **c.** Addresses contingency roles, responsibilities, assigned individuals with contact information;
- **d.** Addresses maintaining essential missions and business functions despite an system disruption, compromise, or failure;
- **e.** Addresses eventual, full systems restoration without deterioration of the controls originally planned and implemented;
- **f.** (P) Addresses resumption of essential missions and business functions within a time frame specified by the BU CIO and based on mission needs, applicable regulations, Arizona State Library, Archives and Public Records requirements and applicable contracts and agreements with external BUs or other organizations. [NIST 800-53 CP-2(3)];
- **g.** (P) Identifies critical assets supporting organizational missions and business functions; [NIST 800-53 CP-2(8)][HIPAA 164.308(a)(7)(ii)(E)]; and
- **h.** (P) Includes procedures for obtaining necessary electronic protected health information during an emergency [HIPAA 164.312(a)(2)(ii)].

6.2 Manage Contingency Plan - The BU shall: [NIST 800-53 CP-2]

- **a.** Distribute the contingency plan to key contingency personnel and organizational elements;
- **b.** Coordinate contingency planning activities with incident handling activities;
- **c.** Review the contingency plan annually;

d. Revise the contingency plan to address changes to the organization, agency systems, operational environment or problems encountered during plan implementation, execution or testing;

e. Communicate contingency plan changes to key contingency personnel and organizational elements; and

f. Protect the contingency plan from unauthorized disclosure and modification.

6.3 (P) **Contingency Plan Coordination** - The BU shall coordinate the development of the contingency plan for each agency system with organizational elements responsible for related plans. [NIST 800-53 CP-2(1)]

6.4 Contingency Training - The BU shall provide contingency training to agency system users consistent with assigned roles and responsibilities before authorizing access, when required by agency system changes, and annually thereafter. The BU shall update and review contingency training content annually and following a major incident. [NIST 800-53 CP-3]

6.5 Test Contingency Plan - The BU shall test the contingency plan for the agency system annually to determine the effectiveness of the plan and the organizational readiness to execute the plan, review the contingency plan test results, and initiate corrective action. [NIST 800-53 CP-4][HIPAA 164.308 (a)(7)(ii)(D)]

6.5.1 (P) **Contingency Plan Test Coordination** - The BU shall coordinate contingency plan testing for each agency system with organizational elements responsible for related plans [NIST 800-53 CP-4(1)] [IRS Pub 1075]

6.6 (P) **Alternate Storage Site** - The BU shall establish an alternate storage site including necessary agreements to permit the storage and recovery of system backup information and ensure that the alternative storage site provides information security safeguards equivalent to those of the primary storage site. [NIST 800-53 CP-6]

6.6.1 (P) **Separation from Primary Storage Site** - The alternative storage site shall be separated from the primary storage site to reduce susceptibility to the same hazards. [NIST 800-53 CP-6(1)] [IRS Pub 1075]

6.6.2 (P) **Accessibility** - The BU shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. [NIST 800-53 CP-6(3)] [IRS Pub 1075]

6.6.3 Arizona State Library, Archive and Public Records is an alternative site by statute (A.R.S. 41-151.12)

6.7 (P) **Alternate Processing Site** - The BU shall: [NIST 800-53 CP-7] [IRS Pub 1075]

a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of agency system operations for essential missions/business functions with the BU's defined time period consistent with recovery time and recovery point objectives when the primary process capabilities are unavailable;

b. Ensure that equipment and supplies to transfer and resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the BU defined period for transfer/resumption; and

c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

6.7.1 (P) **Separation from Primary Site** - The BU shall identify an alternative processing site that is separated from the primary site to reduce susceptibility to the same threats. [NIST 800-53 CP-7(1)] [IRS Pub 1075]

6.7.2 (P) **Accessibility** - The BU shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. [NIST 800-53 CP-7(2)] [IRS Pub 1075]

6.7.3 (P) **Priority of Service** - The BU shall develop alternative processing site agreements that contain priority of service provisions in accordance with the organization's availability requirements. [NIST 800-53 CP-7(3)] [IRS Pub 1075]

6.8 (P) **Alternate Telecommunication Site** - The BU shall ensure alternate telecommunications services are established including necessary agreements to permit the resumption of agency system operations for essential missions and business functions within the BU's defined time period when the primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites. [NIST 800-53 CP-8] [IRS Pub 1075]

6.8.1 (P) **Priority of Service Provisions** - The BU shall ensure primary and alternate telecommunications service agreements are developed that contain priority-of-service provisions in accordance with the BU's availability requirements and requests telecommunication service priority for all telecommunications services used for national or state security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. [NIST 800-53 CP-8 (1)] [IRS Pub 1075]

6.8.2 (P) **Single Points of Failure** - The BU shall ensure alternate telecommunications services are obtained, with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunication services. [NIST 800-53 CP-8(2)] [IRS Pub 1075]

6.9 System Backup - The BU shall: [NIST 800-53 CP-9] [HIPAA 164.308(7)(ii)(A)]

a. Conduct backups of user-level and system-level information contained in the agency system, and agency system documentation including security and privacy related documentation within the BU's defined frequency consistent with recovery time and recovery point objectives; and

b. Protect the confidentiality, integrity, and availability of the backup information.

6.9.1 (P) **Testing for Reliability/Integrity** - The BU shall test backup information at least annually to verify media reliability and information integrity. [NIST 800-53 CP-9(1)] [IRS Pub 1075]

6.9.2 (P) **Cryptographic Protection** - The BU shall Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of BU-defined backup information. [NIST 800-53 CP-9(8)]

6.10 system Recovery and Reconstitution - The BU shall provide for the recovery and reconstitution of the agency system to a known state within the BU-defined recovery time and recovery point objectives after a disruption, compromise, or failure. [NIST 800-53 CP-10]

6.10.1 (P) **Transaction Recovery** - The BU shall implement agency systems to perform transaction recovery for any system that is transaction-based. [NIST 800-53 CP-10(2)] [IRS Pub 1075]

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 8230 Contingency Planning

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

8.6 Establishing an Essential Records List, Arizona State Library, Archives and Public Records

8.7 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number: GS 1005, Arizona State Library, Archives and Public Records, Item Number 7

8.8 A.R.S. 41-151.12

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**
5/26/2021	**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**

STATEWIDE POLICY (8240): INCIDENT RESPONSE PLANNING

DOCUMENT NUMBER:	**P8240**
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 increase the ability of the Budget Unit (BU) to rapidly detect incidents, minimize any loss due to destruction, mitigate the weaknesses that were exploited, and restore computing services.

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 BUs.

5.2 State Chief Information Security Officer (CISO) shall:

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

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing PSPs; and

c. 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 State Chief Privacy Officer (CPO) shall:

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

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

c. Identify and convey to the Director and the State CISO the privacy risk to state systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.4 Enterprise Security Program Advisory Council (ESPAC)

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

5.5 BU Director shall:

a. Be responsible for the correct and thorough completion of (Agency) BU PSPs;

b. Ensure compliance with BU PSPs with Incident Response Planning Policy; and

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

5.6 BU CIO shall:

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

b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements, lessons learned from actual incidents, and advances the industry.

5.7 BU ISO shall:

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

b. Ensure the development and implementation of adequate controls enforcing the Incident Response Planning Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to planning and responding to security incidents.

5.8 BU Privacy Officer shall: [EO 2008-10]

a. Advise the State CISO and the State CPO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with privacy laws, regulations, and statutes; and

b. Assist the agency to ensure the privacy of sensitive personal information within the agency's possession.

5.9 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Incident Response Planning Policy; and

b. Monitor employee activities to ensure compliance.

5.10 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding classification of incidents response planning within agency systems.

6. STATEWIDE POLICY

6.1 **Incident Response Training** - The BU shall provide incident response training to agency system users consistent with assigned roles and responsibilities before authorizing access to the agency system or performing assigned duties, when required by agency system changes, and annually thereafter. The BU shall review and update incident response training content annually and following a major incident. [NIST 800-53 IR-2] [IRS Pub 1075] [PCI DSS 12.10.4]

6.1.1 **Breach** - The BU shall provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach [NIST 800-53 IR-2(3)]

6.2 (P) **Incident Response Testing** – The BU shall test the incident response capability for the agency system annually using checklists, walk-through, tabletop exercises, simulations, or comprehensive exercises to determine the incident response effectiveness and document the results. [NIST 800-53 IR-3] [IRS Pub 1075] [PCI DSS 12.10.2]

6.2.1 (P) **Coordinated Testing** – The BU shall coordinate incident response testing with BU elements responsible for related plans. [NIST 800-53 IR-3(2)] [IRS Pub 1075]

6.2.2 **(P) Incident Response Test Elements** – The BU shall include the following elements (at a minimum) in the annual incident response test: [PCI DSS 12.10.2]

- **a.** Incident response roles and responsibilities, communications, and contact strategies
- **b.** Specific incident response procedures
- **c.** Business recovery and continuity procedures
- **d.** Data back-up processes
- **e.** Legal requirement and breach notification analysis
- **f.** Critical system component coverage and responses
- **g.** Reference or inclusion of Incident response procedures from external entities

6.3 **Incident Handling** - The BU shall implement an incident handling capability for incidents that is consistent with the incident response plan; and [NIST 800-53 IR-4] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)] [PCI DSS 12.10.1]

- **a.** The BU incident response plan shall include preparation, detection and analysis, containment, eradication, and recovery;
- **b.** The BU shall coordinate incident handling activities with contingency planning activities; These activities shall address the following at a minimum:
    1. Unauthorized wireless access point detection [PCI DSS 11.1.2]
    2. Alerts generated by change detection solutions (e.g., unauthorized modification of critical files, configuration files or content files) [PCI DSS 11.5.1]
- **c.** The incident response procedures, training, and testing/exercises shall cover industry developments and lessons learned from ongoing incident handling activities that drive the modification and evolution of the incident response plan; [PCI 12.10.6]industry developments;
- **d.** Implementation of industry development changes where applicable; and
- **e.** The BU shall ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

6.3.1 (P) **Automated Incident Handling Processes** - The BU shall employ automated mechanisms to support the incident handling process. [NIST 800-53 IR-4(1)] [IRS Pub 1075]

6.3.2 (P) **Assign Incident Handling Role** - The BU shall assign to an individual or team the information security management responsibility of implementing an incident response plan and to be prepared to respond immediately to a system breach. [PCI DSS 12.10.1]

6.3.3 (P-PCI) **24x7 Availability** - The BU shall assign to specific personnel the information security management responsibility of being available on a 24x7 basis to respond to alerts. [PCI DSS 12.10.3]

6.3.4 (P) **Forensic Capability** - For agencies that provide a shared hosting service, the BU shall establish processes to provide for timely forensic investigation in the event of a compromise to any hosted service. [PCI DSS A.1.3]

6.4 Incident Monitoring - The BU shall track and document agency system security incidents. [NIST 800-53 IR-5] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)]

6.4.1 (P) **Assign Incident Monitoring Role** - The BU shall assign to an individual or team the information security management responsibility of monitoring and analyzing security alerts and information and distributing alerts to appropriate personnel. [PCI DSS 12.5.2]

6.4.2 (P) **Incorporate Automated Alerts** - The BU shall implement the system to include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems. [PCI DSS 12.10.5]

6.4.3 Continuous Monitoring Strategy - The BU shall develop an BU-wide continuous monitoring strategy and implement continuous monitoring programs that include: [NIST 800 53 PM-31]

- **a.** Establishing the BU-defined metrics to be monitored;
- **b.** Establishing [BU-defined frequency for monitoring and annual assessment of control effectiveness;
- **c.** Ongoing monitoring of BU-defined metrics in accordance with the continuous monitoring strategy;
- **d.** Correlation and analysis of information generated by control assessments and monitoring;
- **e.** Response actions to address results of the analysis of control assessment and monitoring information; and
- **f.** Reporting the security and privacy status of BU systems to the BU CISO, BU Privacy Officer, State CISO and State Privacy Officer annually.

6.5 Incident Reporting - The BU shall require personnel to report: [NIST 800-53 IR-6] [ARS 41-4282] [IRS Pub 1075] [EO 2008-10] [HIPAA 164.308(a)(6)(ii)] [HIPAA 164.308(a)(1)(ii)(D)] [HIPAA 164.314(a)(2)(i)(C)]

- **a.** Suspected security incidents to the organizational incident response capability within one hour of knowledge of suspected incident as specified in the Statewide Standard 8240, Incident Response Planning:
- **b.** (In the event of a security incident) Security incident information to the State CISO; and
- **c.** (In the event of a privacy incident) Privacy incident information to the State Privacy Officer..

6.5.1 Use of Statewide Incident Handling Program – BUs utilizing the statewide incident handling program meet the requirement for reporting of security and privacy incidents that are visible within the program (e.g., part of the monitored systems and logs). However, BUs must implement a system to integrate the notification process for security incidents that originate outside of the monitored systems (e.g., employee reported malware, onsite physical threats, reported loss of laptop).

6.5.2 (P) **Automated Incident Reporting** - The BU shall employ automated mechanisms to assist in the reporting of security incidents. [NIST 800-53 IR-6(1)] [IRS Pub 1075]

6.5.3 (P) **Supply Chain Coordination** - The BU shall provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply **chain** governance for systems of system components related to the incident. [NIST 800-53 IR-6(3)]

6.5.4 (P) **Incident Response Reporting** - the BU shall Respond to information spills by: [NIST 800 53 IR-9]

- **a.** Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;
- **b.** Identifying the specific information involved in the system contamination;
- **c.** Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill;
- **d.** Isolating the contaminated system or system component;
- **e.** Eradicating the information from the contaminated system or component;
- **f.** Identifying other systems or system components that may have been subsequently contaminated; and
- **g.** Performing the additional BU-defined actions.

6.6 Incident Response Plan - The BU shall: [NIST 800-53 IR-8] [IRS Pub 1075] [PCI DSS 12.10, 12.10.1]

- **a.** Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and manage an incident response capability;
8. (P-PCI) Describes the roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, specific incident response procedures, business recovery and continuity procedures, data backup processes, analysis of legal requirements for reporting compromises, coverage and responses of all critical system components, and reference or inclusion of incident response procedures from the payment brands. [PCI DSS 12.10.1]; and
9. Is reviewed and approved by the BU Information Security Officer.
10. Addresses the sharing of incident information;
11. Explicitly designates the responsibility for incident response.
12. (P) Addresses breaches involving personally identifiable information. including: a process to determine if notice to individuals or other organizations, including oversight organizations, is needed; an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and Identification of applicable privacy requirements. [NIST 800-53 IR-8(1)]

b. The BU shall:

1. Distribute copies of the incident response plan to incident response personnel and organizational elements;
2. Review the incident response plan annually;
3. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
4. Communicate incident response plan changes to (Agency) BU incident response personnel and the State CISO and State Privacy Officer; and
5. Protect the incident response plan from unauthorized disclosure and modification.

6.7 Incident Response Assistance - The BU shall provide an incident response support resource, integral to the BU incident response capability that offers advice and assistance to users of the system for the handling and reporting of incidents. [NIST 800-53 IR-7] [IRS Pub 1075]

6.7.1 (P) **Automated Support for Availability of Information** - The BU shall employ automated mechanisms to increase the availability of incident response-related information and support. [NIST 800-53 IR-7(1)] [IRS Pub 1075]

6.8 Investigation - The BU shall promptly investigate potential privacy incidents upon awareness of unencrypted Personally Identifiable Information (PII) loss. [ARS 18-552.A]

a. Breach Determination – The investigation shall determine if the security incident resulted in a system security breach. [ARS 18-552.A]

b. Determination of No Substantial Economic Loss – If an independent third-party forensic auditor or law enforcement agency performed a reasonable investigation and has determined that the system breach has not resulted in or in not reasonably likely to result in substantial economic loss to affected individuals the BU is not required to make the notification as described below. [ARS 18-552.J]

6.9 Notification – The BU shall notify affected parties upon breach determination within 45 days after the determination. [ARS 18-551.B, 18-551.H][HIPAA 164.404(a)]

a. Non-state Owned PII Notification - For PII not owned by the state, the BU shall notify and cooperate with the owner following the discovery of a breach as soon as practicable, including sharing information relevant to the breach. [ARS 18-552.C]

b. Notification Exceptions - The BU may delay or potentially forgo notification in the following cases:

1. if law enforcement determines notification will impede the investigation. The required notification shall be implemented within 45 days of being informed by law enforcement that notifications no would longer impede the investigation, [ARS 18-552.D] [HIPAA 164.412]

2. Good Faith Exposure – No notification is required in the event the disclosure was unintentional or inadvertent by a workforce member acting in good faith and there is no further disclosure. [HIPAA 164.402.1.i-ii]

3. No Retention – No notification is required in the event the disclosure is to an unauthorized person but it is believed that

there is no reasonable way for that person to retain the information. [HIPAA 164.402.1.iii]

4. Low Probability of Compromise – No notification is required in the event the disclosure is demonstrated to have a low probability of compromise based on a risk assessment that considers at least the following factors: [HIPAA 164.402.2]
    i. The nature and extent of the PHI involved (including identifier types, and likelihood of re-identification)
    ii. The unauthorized person to whom the PHI was exposed
    iii. Whether the PHI was actually acquired or viewed; and
    iv. The extent to which the risk to the PHI has been mitigated.
5. If the BU determines a Low Probability of Compromise the determination must be supported through a documented risk analysis process. See Attachment for Example Harm Analysis]

c. Notification Methods - The BU may use written notice via mail, telephone (but not through a prerecorded message), or email as a method of notification. [ARS 18-552.F]
    1. If the cost of notification via these methods would exceed $50,000 the notification method may be a written letter to the attorney general that demonstrates the facts necessary for substitute notice, and a conspicuous posting of the notice for at least 435 days on the BU website. [ARS 18-552.F.4]
    2. If the breach involves account login information (e.g., username and password or security questions) and not any other personal information, the notification may an electronic message that directs the user to re-secure the account (and all other accounts using the same password or security question) by changing the password and security question(s). [ARS 18-551.G]
    3. If the breach involves account login information with an email account the notification may be directed to the individual using a method other than the suspect email address:
        i. Notification delivered online when the IP address or online location matches a known customary address or location for that account. [ARS 18-551.G]

d. (P-PHI) Notification Timing – The BU shall implement notifications without unreasonable delay and in no case later than 45 days after discovery of a breach or suspected breach of PHI. [ARS 18-552.B], [HIPAA 164.404(b), 164.406(b)]

e. Notification Elements – The notification shall include the following elements: [ARS 18-552.E]

1. Approximate date of breach
2. Brief description of personal information included in the breach
3. Toll-free numbers and addresses for the 3 largest nationwide consumer reporting agencies
4. Toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

f. (P-PHI) Additional Notifications – For a breach of unsecured PHI the following additional notifications must be implemented:

1. Breach Log - For breaches involving less than 500 residents of a State or jurisdiction the BU shall maintain a log of such breaches. [HIPAA 164.408(c)].
2. Media Notification - For PHI breaches involving more than 500 residents of a State or jurisdiction the BU shall notify prominent media outlets serving the State or jurisdiction. [HIPAA 164.406(a)].
3. (P-PII) Media Notification – For PII breaches involving more than 1000 individuals notify the 3 largest nationwide consumer-reporting agencies and the attorney general with a copy of the notification provided to the individuals. [A.R.S. 18-552.B.2]
4. HHS Secretary Notification – For any PHI breach the BU shall notify the Secretary of Health and Human Services. In addition each year the BU shall notify the HHS Secretary of the logged data of PHI breaches in the manner specified on the HHS website. [HIPAA 164.408(a), 164.408(b), 164.408(c)].

g. (P) Federal Regulators – A BU is compliant with the notification requirements if they are compliant with the notification requirements established by their primary or functional federal regulator. [ARS 18-552.I]

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 8240 Incident Response Planning

8.2 Statewide Standard 8240, Incident Response Planning

8.3 Statewide Policy Exception Procedure

8.4 Incident Handling Program

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

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

8.7 HIPAA HITECH (Health Information Technology for Economic and Clinical Health) Act February 17, 2010.

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

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

8.10 Executive Order 2008-10: Mitigating Cyber Security Threats, January 14, 2008.

9. ATTACHMENTS

Example Risk of Harm Analysis Procedure:
https://aset.az.gov/resources/policies-standards-and-procedures

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**

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

STATEWIDE POLICY (8250): MEDIA PROTECTION

DOCUMENT NUMBER:	**P8250**
EFFECTIVE DATE:	**January 16, 2024**
REVISION:	**4.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the BU 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 increase the ability of the Budget Unit (BU) to ensure the secure storage, transport, and destruction of sensitive information.

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, (Agency) 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 the BU activities and documentation provided to ensure compliance with 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 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 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Security PSPs within the BU;
b. Ensure BU compliance with Media Protection Policy; and
c. Promote efforts within the BU to establish and maintain effective use of agency systems and assets.

5.5 BU CIO shall:

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

b. Ensure Media Protection PSPs are periodically reviewed and updated.

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 and implementation of an adequate controls enforcing Media Protection PSPs for the BU;

c. Request changes and/or exceptions to existing Media Protection PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to protection of removable media in connection with agency systems and premises.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Media Protection Policies; and

b. Monitor employee activities to ensure compliance.

5.8 Users of agency systems shall:

a. Familiarize themselves with this policy and related PSPs; and

b. Adhere to PSPs regarding protection of removable media in connection with agency systems and premises.

6. STATEWIDE POLICY

6.1 **Media Access** - The BU shall restrict access to digital and non-digital media to authorized individuals. [NIST 800-53 MP-2] [HIPAA 164.308(a)(3)(ii)(A)] [PCI DSS 9.6] [IRS Pub 1075]

6.2 (P) **Media Marking** - The BU shall mark, in accordance with BU policies and procedures, system digital and non-digital media containing Confidential information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information, as well as exempt removable digital media from marking as long as the exempted items remain with a controlled environment. [NIST 800-53 MP-3] [PCI DSS 9.6.1] [IRS Pub 1075]

6.3 (P) **Media Storage -** The BU shall physically control and securely store digital and non-digital media containing Confidential information within controlled areas. [NIST 800-53 MP-4] [ARS 39-101] [PCI DSS 9.5] [PCI DSS 9.7] [IRS Pub 1075]

6.4 (P) **Media Inventories -** The BU shall maintain inventory logs of all digital media containing Confidential information and conduct inventories annually. [PCI DSS 9.7.1]

6.5 (P) **Media Transport –** The BU shall protect and control digital and non-digital media containing Confidential information during transport outside controlled areas. [NIST 800-53 MP-5] [PCI DSS 9.6] [IRS Pub 1075]

6.5.1 (P) **Cryptographic Protection -** The BU shall employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas. Cryptographic mechanisms must comply with System and Communication Protection Standard S8350. [NIST 800-53 SC-28(1)] [HIPAA 164.312(c)(2)] [IRS Pub 1075]

6.5.2 (P-PHI) **Media Transport Policies** - The BU shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential information into and out of a protected facility, and the movement of these items within the facility. [HIPAA 164.310(d)(1)]

6.5.3 (P) **Secure Delivery -** The BU shall send confidential digital and non-digital media by secured courier or other delivery method. [PCI DSS 9.6.2]

6.5.4 (P-PHI) **Record of Movement -** The BU shall maintain a record, including the person(s) responsible, of the movements of hardware and digital media. [HIPAA 164.310(d)(2)(iii)]

6.5.4.1 (P) **Data Backup -** The BU shall create a retrievable, exact copy of Confidential data, when needed before movement of equipment. [HIPAA 164.310(d)(2)(iv)]

6.5.4.2 (P) **Backup Storage -** The BU shall store digital media backups in a secure location and review the location's security, at least annually. [PCI DSS 9.5.1]

6.5.5 (P) **Management Approval -** The BU shall ensure management approves any media that is moved from a controlled area. [PCI DSS 9.6.3]

6.6 Media Sanitization - The BU shall sanitize digital and non-digital system media containing Confidential information prior to disposal, release of organizational control, or release for reuse using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250. [NIST 800-53 MP-6] [HIPAA 164.310(d)(2)(i)] [HIPAA 164.310(d)(2)(ii)] [IRS Pub 1075] [PCI DSS 9.8, 9.8.1, 9.8.2]

6.6.1 Secure Storage - Secure storage containers used for materials that are to be destroyed. [PCI DSS 9.8.1]

6.6.2 (P-FTI) **Verify Sanitization** - The BU shall review, approve, track, document, and verify media sanitization and disposal actions. [NIST 800-53 MP-6(1)] [IRS Pub 1075]

6.7 Media Use – The BU shall restrict the use of [BU-specified type of digital media] on [BU-specified agency systems and/or system components] and prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.. [NIST 800-53 MP-7] [IRS Pub 1075]

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 P8250 Media Protection

8.2 Statewide Policy Exception Procedure

8.3 Statewide Standard S8250, Media Protection

8.4 System and Communication Protection, Standard S8350

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

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

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

8.8 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**

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

STATEWIDE POLICY (8260): PHYSICAL SECURITY PROTECTIONS

DOCUMENT NUMBER:	**P8260**
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 as authorized by Arizona Revised Statutes (A.R.S.) § 18-104 and § 18-105.

2. PURPOSE

The purpose of this policy is to protect agency systems and assets through limiting and controlling physical access and implementing controls to protect the environment in which agency systems and assets are housed.

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 Policies, Standards and Procedures (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 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 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Security PSPs within the (Agency) BU;

b. Ensure BU compliance with Physical Protections Policy; and

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

5.5 BU 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 Physical Security Controls Policy is 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 Agency Information Security PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the Physical Protections Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the physical protection of agency systems and assets.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Physical Protections Policies; and

b. Monitor employee activities to ensure compliance.

5.8 Users of agency systems shall:

a. Familiarize themselves with this policy and related PSPs; and

b. Adhere to PSPs regarding the physical protection of agency systems and assets.

6. STATEWIDE POLICY

6.1 Physical Access Authorizations - The BU shall: [NIST 800-53 PE-2] [IRS Pub 1075] [HIPAA 164.310 (a)(2)(iii)] [PCI DSS 9.9, 9.3]

a. Develop and maintain a list of individuals with authorized access to controlled areas or facilities where the agency system resides;

b. Issue authorization credentials based on job function; [PCI DSS 9.3]

c. Review and approve the access list and authorization credentials quarterly; and

d. Remove individuals access (including from the access list, keys, badges, and combination changes) when access is no longer required and immediately upon termination. [PCI DSS 9.3]

6.2 Standard Physical Access Control - The BU shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. Enforce physical access authorization at designated entry/exit points to the facility where the agency system resides; [PCI DSS 9.1]

b. Verify individual access authorizations before granting access to the facility; [PCI DSS 9.1, 9.3.1]

c. Control ingress and egress to the facility using keys, locks, combinations, badge readers, and/or guards;

d. Maintain physical access audit logs for BU-defined entry and exit points;

e. Control access to areas within the facility designated as publicly accessible by implementing BU-defined controls; and

f. (P-PCI) Provide cameras, monitoring by guards, or isolating selected agency system components (or any combination) to control access to areas within the facility officially designated as publically accessible. Review collected data and correlate with other entries. Store at least three (3) months unless otherwise directed by law. [PCI DSS 9.1.1]

6.3 Protected Physical Access Control - For all Protected agency systems and the server components of standard agency systems for which additional physical protections apply, the (Agency) BU shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. (P) Develop procedures to identify and authorize visitors [PCI DSS 9.4]

b. (P) Develop procedures to easily distinguish between onsite personnel and visitors. [PCI DSS 9.2];

c. (P) Give visitors a physical token that expires and that identifies the visitors as onsite personnel and ensure the visitor surrenders the physical token before leaving the facility or at the date of expiration; [PCI DSS 9.4.2, 9.4.3.]

d. Escort visitors and monitors visitor activity within controlled areas; [NIST 800-53 PE-3.d] [PCI DSS 9.4.1]

e. Secure keys, combinations, and other physical access devices;

f. Inventory keys and other physical access devices every quarter; keys and other physical access devices assigned to visitors are inventoried every day; and

g. Change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or separated.

6.4 Monitoring Physical Access - The BU shall: [NIST 800-53 PE-6] [IRS Pub 1075]

a. Monitor physical access to the agency system to detect and respond to physical security incidents;

b. (P) Use video cameras and/or access control mechanisms (or both) to monitor physical access to sensitive areas. [PCI DSS 9.1.1]

c. (P) Review physical access logs weekly and, upon occurrence of potential indications of events; [PCI 9.1.1]

d. (P) Coordinate results of reviews and investigations with the organizational incident response capability; and

e. (P) Store physical access monitoring data for at least three months. [PCI 9.1.1]

6.4.1 (P) **Intrusion Alarms and Surveillance Equipment** - The BU shall monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment. [NIST 800-53 PE-6(1)] [IRS Pub 1075]

6.4.2 (P-PCI) Inspect Payment Card Capture Devices - Periodically inspect device surfaces to detect tampering or substitution (for example, addition of card skimmers to devices, unexpected attachments or cables plugged into the device, missing, changed security labels, different colored casing, or changes to the serial number or other external markings). [PCI 9.9.2]

6.5 Visitor Control Records - The BU shall: [NIST 800-53 PE-8] [PCI DSS 9.4.4]

a. Maintain visitor access records to the controlled areas or facilities where the system resides for a minimum of three months; [PCI 9.1.1]

b. Review visitor access records monthly and report anomalies in visitor access records to appropriate personnel;

c. Maintain a visitor log that includes the visitor's name, the firm represented, and the onsite personnel authorizing physical access.

6.5.1 **Limit Personally Identifiable Information Elements** - The BU shall limit personally identifiable information collected in visitor access records to the BU-defined elements identified in the system privacy risk assessment; [NIST 800-53 PE-8(3)]

6.6 (P) **Access Control** - The BU shall implement the following physical access controls:

6.6.1 (P) **Transmission Medium** - The BU shall control physical access to agency system distribution and transmission lines within BU facilities using locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays. [NIST 800-53 PE-4] [IRS Pub 1075]

6.6.2 (P) **Workstations** -The BU shall implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users. [HIPAA 164.310(b), 164.310(c)]

6.6.3 (P) **Output Devices** - The BU shall control physical access to BU-defined agency system output devices to prevent unauthorized individuals from obtaining output. [NIST 800-53 PE-5] [IRS Pub 1075]

6.6.4 (P-PCI) **Network Jacks and Devices** - The BU shall restrict physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. [PCI 9.1.2, 9.1.3]

6.6.5 (P) **Power Equipment and Cabling** - The BU shall protect power equipment and power cabling for the agency system from damage and destruction. [NIST 800-53 PE-9]

6.7 (P) **Power -** The BU shall implement the following physical controls for power:

6.7.1 (P) **Emergency Shutoff** - The BU shall: [NIST 800-53 PE-10]

a. Provide the capability of shutting off power to the BU-defined system or individual system components in emergency situations;

b. Place emergency shutoff switches or devices in data centers, server rooms, and computer rooms to facilitate safe and easy access for personnel; and

c. Protect emergency power shut off capability from unauthorized activation.

6.7.2 (P) **Emergency Power** - The BU shall provide an uninterruptible power supply to facilitate an orderly shutdown of the system or a transition of the system to long-term alternate power in the event of a primary power source loss. [NIST 800-53 PE-11]

6.8 Emergency Lighting - The BU shall employ and maintain automatic emergency lighting for the agency system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. [NIST 800-53 PE-12]

6.9 Fire Protection - The BU shall employ and maintain fire detection and suppression that are supported by an independent energy source. [NIST 800-53 PE-13]

6.9.1 (P) **Detection Devices** - The BU shall employ fire detection systems that activate automatically and notify the BU and emergency responders in the event of a fire. [NIST 800-53 PE-13(1)]

6.9.2 (P) **Suppression Devices** - The BU shall employ fire suppression systems that activate automatically and notify the BU and emergency responders and employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.[NIST 800-53 PE-13(2)]

6.9.3 (P) **Inspections** - The BU shall ensure the facility undergoes annual inspections by authorized and qualified inspectors and resolves identified deficiencies within 30 days. [NIST 800-53 PE-13(4)]

6.10 Temperature and Humidity Controls - The BU shall maintain defined temperature and humidity levels within the facility where the system resides at data centers, server rooms and computer rooms; and monitors temperature and humidity levels daily. [NIST 800-53 PE-14]

6.11 Water Damage Protection - The BU shall protect systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. [NIST 800-53 PE-15]

6.12 Delivery and Removal - The BU shall authorize and control systems components entering and exiting the facility and maintains records of those system components. [NIST 800-53 PE-16]

6.13 (P) **Alternate Work Site** - The BU shall: [NIST 800-53 PE-17]

a. Determine and document the alternative work sites allowed for use by employee;

b. Define and employ minimum controls at alternate work sites;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of security incidents.

6.14 (P) **Location of System Components** - The BU shall position system components within the facility to minimize potential damage from BU-defined physical and environmental hazards and to minimize the opportunity for unauthorized access. [NIST 800-53 PE-18]

6.15 (P) **Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for restricting physical access are documented, in use, and known to all affected parties [PCI DSS 9.10]

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 P8260 Physical Protections

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.

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**

	STATEWIDE # POLICY	**State of Arizona**

STATEWIDE POLICY (8270): PERSONNEL SECURITY CONTROLS

DOCUMENT NUMBER:	**P8270**
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 increase the ability of the Budget Unit (BU) to protect agency systems and assets containing sensitive data through personnel security controls.

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 - 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 - 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 BUs.

5.2 State Chief Information Security Officer (CISO) shall:

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

b. Review and approve all state 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 The 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 security PSPs;
- **b.** Ensure the development and implementation of an adequate controls enforcing the Personnel Security Policy for the BU;
- **c.** Ensure all personnel understand their responsibilities with respect to the protection of agency systems and assets through personnel security controls.

5.7 Supervisors of agency employees and contractors shall:

- **a.** Ensure users are appropriately trained and educated on Personnel Security Policies; and
- **b.** Monitor employee activities to ensure compliance.

5.8 Users of agency systems shall:

- **a.** Familiarize themselves with this and related PSPs; and
- **b.** Adhere to PSPs regarding the protection of agency systems and assets through personnel security controls.

6. STATEWIDE POLICY

6.1 Position Categorization - The BU shall:

a. Assign a sensitivity designation (e.g., Sensitive, Non-Sensitive) to all positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and revise position sensitivity designations annually. Sensitivity designations are based on the individual's exposure to sensitive system information and/or administrative privileges to agency systems. Examples of sensitive positions include: [NIST 800-53 PS-2] [IRS Pub 1075]

1. Firewall administrator;

2. Members of the incident response team; and

3. Those with vulnerability scanning duties.

6.2 Position Definition - The BU shall define information security and privacy responsibilities for all personnel. [HIPAA(a)(3)(ii)(A), (a)(3)(ii)(B) - Addressable] [PCI DSS 12.4, 12.5]. [NIST 800-53 PS-9] Specifically, the following information security and privacy responsibilities:

a. Individual or team responsible for establishing, documenting, and distributing security and privacy policies and procedures; [PCI DSS 12.5.1]

b. Individual or team responsible for monitoring and analyzing security and privacy alerts and information, and distributing to appropriate employees and contractors; [PCI DSS12.5.2]

c. Individual or team responsible for establishing, documenting, and distributing security and privacy incident response and escalation procedures to ensure timely and effective handling of all situations; [PCI DSS 12.5.3]

d. Individual or team responsible for administering user accounts, including additions, deletions, and modifications; and [PCI DSS 12.5.4]

e. Individual or team responsible for monitoring and controlling all access to data. [PCI DSS 12.5.5]

6.3 Personnel Screening - The BU shall screen individuals holding positions designated as sensitive prior to hiring or contracting; and rescreens individuals according to re-screening every three years. [NIST 800-53 PS-3] [IRS Pub 1075] [PCI DSS 12.7]

6.4 Personnel Separation - Upon separation of individual employment, the BU shall: [NIST 800-53 PS-4] [HIPAA(a)(3)(ii)(C)]

a. Disable agency system access within 24 hours;

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews, if employee is available for interview;

d. Retrieve all security-related agency system-related property;

e. Retain access to agency information and system accounts formerly controlled by separated individual; and

f. Allow the separated individual access to authorized services such as benefits, reimbursement, and retirement information, according to (Agency) BU or State policies.

6.5 Personnel Transfer - The BU shall: [NIST 800-53 PS-5] [IRS Pub 1075]

a. Review logical and physical access authorization to agency systems/facilities when personnel are reassigned or transferred to other positions within the organization;

b. initiates returning old and reissuing new keys, identification cards, and building passes within 24 hours;

c. Close previous system accounts and establish new accounts and changes agency system access authorizations;

d. Provide access to official records to which the employee had access at the previous work location and in the previous agency system accounts within 24 hours; and

e. The (Agency) BU may extend limited access for special purposes on an exception basis.

6.6 Access Agreements - The BU shall: [NIST 800-53 PS-06] [IRS Pub 1075] [PCI DSS 12.3].

a. Develop and document access agreements for agency systems;

b. Review and update the access agreements annually;

c. Verify that individuals requiring access to agency information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or annually.

Third-Party Personnel Security - The BU shall: [NIST 800-53 PS-7] [IRS Pub 1075] [HIPAA 164.314(a)(1)]

a. Establish personnel security requirements including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the agency;

c. Document personnel security requirements; and

d. Require external providers to notify BU-defined personnel of any personnel transfers or terminations of external personnel who posses organizational credentials and/or badges, or who have system privieges with 24 hours; and

e. Monitor provider compliance.

6.7 Third-Party Contracts - The BU shall ensure that third party contractors specify the third-party will: [HIPAA 164.314(a)(2)(i)]

a. Comply with the applicable security requirements;

b. Ensure that any subcontractors that create, receive, maintain, or transmit sensitive information on behalf of the third-party agree to comply with applicable requirements; and

c. Report to the BU any security incident of which it becomes aware, including breaches of unsecured sensitive information.

6.8 Personnel Sanctions - The BU shall employ a formal sanctions process for personnel failing to comply with established agency information security and privacy PSPs and document the sanctions applied. [NIST 800-53 PS-8] [IRS Pub 1075] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]

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 P8270 Personnel Security Controls

8.2 Statewide Policy Exception Procedure

8.3 Executive Order 1403

8.4 A.R.S. 41-710

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

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

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

8.8 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**

STATEWIDE POLICY (8280): ACCEPTABLE USE

DOCUMENT NUMBER:	**P8280**
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 (ARS)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of agency system assets to reduce the risks to agency systems due to disclosure, modification, or disruption, whether intentional or accidental.

3. SCOPE

3.1 **Application to Budget Unit (BU)** - 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. Policy statements preceded by "(P)" are required for agency systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

3.3 **Application to End User** - The content of this policy is primarily focused towards the end-user, unless explicitly specified otherwise, as stated in Section 3.1.

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 - 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 - 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 BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of all state BU activities and documentation provided to ensure compliance with S

b. Statewide information security PSPs throughout all state BUs;

c. Review and approve BU security and privacy PSPs and requested 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 the 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 BU Director shall:

a. Be responsible for the correct and thorough completion of (Agency) BU PSPs;

b. Ensure compliance with BU PSPs; and

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

5.5 BU CIO shall:

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

b. Ensure the Acceptable Use Policy is 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 information security PSPs;

b. Ensure the development and implementation of adequate controls enforcing the BU PSPs;

c. Request changes and/or exceptions to existing Statewide PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to acceptable use of agency systems and assets.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on acceptable use policies; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this and related PSPs; and

b. Adhere to PSPs regarding classification of data and handling within agency systems.

6. STATEWIDE POLICY

6.1 **Access Agreements** - The BU Director shall ensure that individuals requiring access to organizational information and agency systems acknowledge and accept appropriate

access agreements (prior to being granted access) and shall review and, if necessary, update the access agreements annually. [NIST 800-53 PS-6] [PCI DSS 12.3].

6.1.1 Rules of Behavior - The BU shall: [NIST 800-53 PL-4]

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are reviewed or updated.

6.1.2 Assign Responsibility to Provide Policy - The BU Director shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

6.1.3 Assign Responsibility to Keep Records - The BU Director shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.2 Access Agreement Contents - The access agreements shall contain the following policy sections and statements:

6.2.1 Expected Behaviors - The following behaviors shall be required:

6.2.1.1 Practice Safe Computing - Those accessing agency systems shall use caution and exercise good security practices to ensure the protection of agency systems and data, including, but not limited to:

e. Opening Attachments or Links - Use caution when opening email attachments or following hypertext links received from unknown senders.

f. Keep Passwords Secure - Select strong passwords, do not write them down, change them frequently, and do not share them with anyone.

g. Keep Desk and Workstation Secure - Use available operating system functions to lock the workstation when away from the desk. At the end

of the day, log out of the computer, but leave the equipment powered on.

h. **Challenge Unauthorized Personnel** - Assist in enforcing physical access controls by challenging unauthorized personnel who may not be following procedures, appropriate badge display and use, escort control, and/or entry.

i. **Report Security or Privacy Weaknesses or Violations** - Report any weaknesses in computer security or data privacy, suspicious behavior of others and any incidents of possible misuse or violation of this policy to the proper authorities.

j. **Wear Issued Badges –** All employees and contractors are required to wear their agency-issued ID badges, while in the building, at all times.

6.2.1.2 Protect Confidential Information - Confidential information shall be protected in accordance with applicable statutes, rules, policies, standards, and procedures. Those accessing agency systems shall protect confidential information in accordance with the STATEWIDE POLICY FRAMEWORK 8110, Data Classification and Handling. Specifically, the following:

6.2.1.3 Marking of Confidential Information - All non-public data must be marked (labeled) as Confidential. Unlabeled data is assumed to be Public.

6.2.1.4 Unencrypted Confidential Information - Confidential information sent over email or other electronic messaging without adequate encryption shall be prohibited (even to an authorized user).

6.2.1.5 Storage of Confidential Information - Confidential information must be stored in accordance with the STATEWIDE POLICY FRAMEWORK 8250, Media Protection.

6.2.1.6 Electronic Transmission of Confidential Information - Confidential information that is transmitted outside of the agency system or on any medium that can be accessed by authorized users shall be encrypted through link or end-to-end encryption with an encryption algorithm and key length that meets the Statewide Standard 8350, System and Communication Protection.

6.2.2 Prohibited Behaviors -The following behaviors shall be prohibited:

a. **Computer Tampering** - Unauthorized access, interception, modification or destruction of any computer, computer system, agency system, computer programs or data; [ARS 13-2316.1-2]

b. **Use of Unauthorized Computing Equipment** - Installation or connections of any computing equipment not provided or authorized by management to agency systems;

c. **Use of Unauthorized Software or Services** - Installation or use of any unauthorized software, including but not limited to browser applications and extensions, security testing, monitoring, encryption, or "hacking" software on agency computing resources; [NIST 800 53 CM-11]

d. **Unauthorized Use of Software or Services** - Use of peer-to-peer file sharing technology used for the unauthorized distribution, display, performance, or reproduction of copyrighted work; [NIST 800 53 CM-10]

e. **Violation of Copyright Law -** Use of software and associated documentation in violation of contract agreements and copyright laws; [NIST 800-53 CM-10]

f. **(P-FTI) Use of Open-Source software -** The use of open-source software in violation of the BU-defined restrictions on the use of open-source software; [NIST CM-10(1)];

g. **Introduction of Malware** - Knowingly introducing a computer contaminant into any computer, computer system or agency system; [ARS 13-2316.3]

h. **System Disruption** - Recklessly disrupting or causing the disruption of a computer, computer system or agency system; [ARS 13-2316.4]

i. **Circumvention of Security Controls** - Disabling software, modifying configurations, or otherwise circumventing security controls. [ARS 13-2316] Tampering with physical security measures (e.g., locks, cameras) is also prohibited;

j. **False Identity** - Falsifying identification information or routing information so as to obscure the origins or the identity of the sender, or using or assuming any system or application identification other than your own;

k. **Cryptocurrency Mining** - Malicious software introduced onto a computer, and power is used to compute math problems to obtain cryptocurrency.

6.2.2.1 Unauthorized Inappropriate or Unlawful Material - The unauthorized storage, transmission, or viewing of any pornography or other offensive, intimidating, hostile or otherwise illegal material is forbidden. Except to the extent required in conjunction with a bona fide agency approved

research project or other agency approved undertaking, an employee of an agency shall not knowingly use agency owned or agency leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sex acts; [ARS 38-448] [ARS 13-2316.5]

6.2.2.2 Unauthorized Use of Electronic Messaging - The following use of electronic messaging shall be prohibited:

- **a. Spam** - Sending of unsolicited commercial emails/electronic messages in bulk (identical content to multiple recipients).
- **b. Chain Letters** - Creating of forwarding chain letters of pyramid schemes.
- **c. Unprofessional Communications** - Unprofessional or un-businesslike in appearance or content.
- **d. Alter Message Content** - Modification or deletion of email/electronic messages originating from another person or computer with the intent to deceive.
- **e. False Identity** - Falsifying email/electronic message headers or routing information so as to obscure the origins of the email/electronic message or the identity of the sender, also known as spoofing.
- **f. Mask Identity** - Unauthorized use of anonymous addresses for sending and receiving email/electronic messages.
- **g. Auto-Forward to External Accounts** - Automatically forwarding email/electronic messages sent to an BU account to an external email/electronic messages without authorization.
- **h. Non-agency Email Accounts** - Unauthorized use of a non-agency email account for agency business.
- **i. Unencrypted Confidential Information** - Confidential information sent over email or other electronic messaging without adequate encryption (even to an authorized user).
- **j. Misrepresentation of BU** - Presenting viewpoints or positions not held by the BU as those of the BU or attributing them to the BU.

6.2.2.3 Personal Use of Agency systems - Personal use of agency technology assets/systems shall be limited to occasional use during break periods provided the use does not interfere with agency systems or services.

6.2.2.4 Social Media and External Site - BU-defined restrictions on the use of the following: [NIST 800-53 PL-4(1)]

a. social media, social networking sites, and external sites and applications,

b. unauthorized posting of BU information on public websites, and

c. the use of BU identifiers (e.g., email address) and authentication secrets for creating accounts on external sites or applications.

6.2.2.5 Violation of Intellectual Property Laws - Unauthorized receipt, use or distribution of unlicensed software, copyrighted materials, or communications of proprietary information or trade secrets.

6.2.2.6 Unauthorized Access of Confidential Information - Unauthorized access of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized access of any confidential information is prohibited. [ARS 13-2316.07]

6.2.2.7 Unauthorized Release of Confidential Information - Disclosure of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized release or disclosure of any confidential information is prohibited. [ARS 36-342] [ARS 36-666] [ARS 41-151.12] [ARS 41-1750.01]

6.2.2.8 Unauthorized Posting of Agency Information or Documents - Unauthorized posting of agency information, draft or final agency documents on public or agency websites or other external sharing is prohibited.

6.2.3 Notifications and Acknowledgements - The following notifications and acknowledgements shall be used to inform those granted access to organizational information and/or agency systems of steps the BU may take to ensure the security of agency systems:

6.2.3.1 User Responsibility Acknowledgement - All users review and acknowledge their understanding of this policy and other related information security policies on an annual basis; [PCI DSS 12.6.2]

6.2.3.2 Assets and Intellectual Property - All agency system assets remain the sole property of the State of Arizona. Any data or intellectual property created by the user, including voicemail and electronic messages, shall remain the property of the State of Arizona and shall not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities;

6.2.3.3 Monitoring - The BU shall inform all users that it reserves the right to monitor all activities that occur on its agency systems or to access any data residing on its systems or assets at any time without further notice. The BU shall retain the right to override an individual's passwords and/or codes to facilitate access by the BU;

6.2.3.4 Potential Blocking of Inappropriate Content - The BU may block access to web content it deems as inappropriate or filter email destined for your mailbox;

6.2.3.5 Incomplete Blocking of Inappropriate Content - The BU shall not be responsible for material viewed or downloaded by users from the Internet or messages delivered to a user's mailbox. Users are cautioned that many Internet pages and emails include offensive, sexually explicit, and inappropriate material. Even though the BU intends to filter and block inappropriate content and messages it is not possible to always avoid contact with offensive content on the Internet or in your email. If such an action occurs users are expected to delete the offensive material, leave the offensive site and contact the BU security department;

6.2.3.6 Records Retention - Files, emails, attachments and other records are retained, preserved, and/or disposed of in accordance with BU records retention policies and in full accordance with the Arizona State Library Records Retention Schedule, Electronic Communication Records: http://apps.azlibrary.gov/records/general_rs/Electronic%20Communications,%20Social%20Networking%20&%20Website.pdf;

6.2.3.7 No Expectation of Privacy - Users shall have no expectation of privacy for any communication or data created, stored, sent, or received on agency systems and assets; and

6.2.3.8 User Acknowledgement - By using agency systems, users shall acknowledge that they explicitly consent to the monitoring of such use and the right of the BU to conduct such monitoring.

6.3 Virtual Office Agreement - The BU shall ensure that individuals utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency systems as a trusted user acknowledge and accept appropriate access agreements prior to being granted access and shall review, and if necessary, update agreements annually.

6.3.1 Assign Responsibility to Provide Policy - The BU shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

6.3.2 Assign Responsibility to Keep Records - The BU shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.4 Virtual Office Access Agreement Contents - The Virtual Office Access agreements shall contain the following additional policy sections and statements:

6.4.1 (P) **Allowable Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency systems as a trusted user providing and storing Confidential information shall ensure:

- **a.** The computing equipment is issued to the individual by the agency for the purposes of connecting to a agency system; or
- **b.** The computing equipment is owned or otherwise under the control of the individual such that the individual may ensure minimum physical and logical protections are in place.

6.4.2 (P) **Physical Protection of Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency systems as a trusted user providing and storing Confidential information shall ensure that computer equipment is:

- **a.** Physically protected from unauthorized use and removal; and
- **b.** Limited to the use of the authorized virtual office user. Use of the computer equipment by anyone else (e.g., family members, roommates) is strictly forbidden.

6.4.3 (P) **Logical Protection of Computing Devices** - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency systems as a trusted user providing and storing Confidential information shall ensure that computer equipment has the following logical security controls:

- **a. Username and Passwords** - Identification and authentication controls consistent with STATEWIDE POLICY FRAMEWORK 8340, Identification and Authentication;
- **b. Anti-Virus** - Malicious code protection consistent with STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance, with the exception of central management of malicious code protection;
- **c. Personal Firewalls** - Personal firewalls consistent with STATEWIDE POLICY FRAMEWORK 8320, Access Control;

d. **Device Encryption** - Full Device Encryption consistent with the Access Control Policy; and

e. **Security Patches** - Install security-relevant software and firmware updates consistent with STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance.

6.4.4 **Remote Access** - Virtual office users may access the agency system only by approved access methods.

6.5 **User-Based Technologies** - The BU shall ensure that individuals utilizing user-based technologies (e.g., smart phones, tablet computers) to access agency systems as a trusted user acknowledge and accept appropriate access agreements (prior to being granted access), and shall review, and if necessary, update agreements annually.

6.5.1 **Assign Responsibility to Provide Policy** - The BU shall assign responsibility to a department, role, or named individual to provide user-technology standards, acceptable use, and other related information security policies to employees and contractors.

6.5.2 **Assign Responsibility to Keep Records** - The BU shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.6 **User-Based Technology Agreement Contents** - The user-based technology access agreements shall be developed by the BU and contains BU-defined security controls. Statewide Standard 8220, System Security Maintenance provides guidance to BU for minimum recommended user-based technology controls. Such agreements shall include the following, at a minimum: [PCI DSS 12.3]

a. Explicit approval by authorized parties [PCI DSS 12.3.1]

c. Authentication for use of the technology [PCI DSS 12.3.2]

d. A list of all such devices and personnel with access [PCI DSS 12.3.3]

e. A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) [PCI DSS 12.3.4]

f. Acceptable uses of the technology [PCI DSS 12.3.5]

g. Acceptable network locations for the technologies [PCI DSS 12.3.6]

h. List of BU-approved products [PCI DSS 12.3.7]

i. Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity [PCI DSS 12.3.8]

j. Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use [PCI DSS 12.3.9]

k. For personnel accessing Confidential data via remote-access technologies, prohibit the copying, moving, and storage of Confidential data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable requirements [PCI DSS 12.3.10]

6.7 Consequences for Non-compliance - Users of agency systems who fail to comply with established information security and privacy policies and procedures may be subject to sanctions, including referral to a law enforcement agency for appropriate action. [NIST 80053 PS-8] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]

6.7.1 Agency Employees - State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct, requires that all employees comply with federal and state laws and rules, statewide policies and employee handbook and agency policy and directives. As provided by SPS Rule R2-5A-501(C), an employee who fails to comply with standards of conduct requirements may be disciplined or separated from state employment.

6.7.2 Agency Contractors - Agency contractors violating federal and state laws and rules, statewide policies, and agency policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.

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 P8280 Acceptable Use

8.2 STATEWIDE POLICY FRAMEWORK 8120, Information Security Program Policy

8.3 Statewide Policy Exception Procedure

8.4 State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct

8.5 Statewide Standard 8350, System and Communication Protection

8.6 Statewide Standard 8220, System Security Maintenance

8.7 STATEWIDE POLICY FRAMEWORK 8340, Identification and Authentication

8.8 STATEWIDE POLICY FRAMEWORK 8320, Access Control

8.9 STATEWIDE POLICY FRAMEWORK 8250, Media Protection

8.10 STATEWIDE POLICY FRAMEWORK 8110, Data Classification and Handling

8.11 STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance

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

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

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

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

8.16 General Records Retention Schedule for All Public Bodies, Electronic Communications, Social Networking and Website Records, Schedule Number 000-12-22, Arizona State Library, Archives and Public Records

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**

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

STATEWIDE POLICY (8310): ACCOUNT MANAGEMENT

DOCUMENT NUMBER:	**P8310**
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.)§ 18-104 and § 18-105.

2 PURPOSE

The purpose of this policy is to establish the baseline controls for the administration of agency system accounts.

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 BUs.

5.2 State Chief Information Security Officer (CISO) shall:

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

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing PSPs; and

c. 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 BU Director shall:

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

b. Ensure compliance with BU PSPs; and

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

5.5 BU CIO shall:

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

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

5.6 BU ISO shall:

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

b. Ensure the development and implementation of adequate controls enforcing the BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to secure account management.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding account management and acceptable use of agency systems.

STATEWIDE POLICY

6. The BU shall implement account management through the following activities:

6.1. (P) **Automated Account Management** - The BU shall support the management of system accounts using automated mechanisms. [NIST 800-53 AC-2(1)] [IRS Pub 1075]

6.2. (P) **Develop Account Management Operational Procedures** - The BU shall ensure that security policies and operational procedures for restricting access to Confidential data are documented, in use, and known to all affected parties and cover all system components. [PCI DSS 7.2.1, 7.3]

6.3. **Identify Account Types** - The BU shall define and document the types of agency system accounts (e.g., individual, guest, emergency access, developer, maintenance, administration) allowed and specifically prohibited for use within the system. . [NIST 800-53 AC-2a] [HIPAA 164.312 (a)(2)(iii) – Addressable] [PCI DSS 7.2.2]

6.3.1. **Establish Group and Role-based Accounts** - The BU shall require BU-defined prerequisites and criteria for group and role membership. [NIST 800-53 AC-2c] [PCI DSS 7.1.1] [PCI DSS 7.2.2]

6.3.2. **Account Specification** -The BU shall specify authorized users of the agency system, group and role membership, and access authorizations (i.e., privileges) and other BU-defined attributes for each account. [NIST 800-53 AC-2d] [PCI DSS 7.1.3]

6.3.3. (P) **Privileged Accounts** - The BU shall restrict privileged accounts (e.g., super user accounts) on the agency system to administrative roles. [NIST 800-53 AC-6(5)] [IRS Pub 1075] [PCI DSS 7.1.2]

6.3.4. (P) **Separation of Duties** - The BU shall identity and document (Agency) BU -defined duties of individuals requiring separation and and define agency system access authorizations to support separation of duties. [NIST 800-53 AC-5] [IRS Pub 1075] [PCI DSS 6.4.2]

6.4. **Assign Account Managers** - The BU shall assign account managers for agency systems. [NIST 800-53 AC-2b]

6.5. Account Approval - The BU shall require documented approvals by authorized BU staff for requests to create, modify, and enable agency system accounts. [NIST 800-53 AC-2e-f] [PCI DSS 7.1.4]

6.5.1. (P) **Automated Audit Actions** - The BU shall ensure the agency system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required, BU-defined personnel or roles. [NIST 800-53 AC-2(4)] [IRS Pub 1075]

6.6. Account Monitoring - The BU shall authorize, and monitor the use of agency system accounts. [NIST 800-53 AC-2g]

6.6.1. (P) **Vendor Account Monitoring** - The BU shall enable accounts used by vendors for remote access only during the time period needed and monitors the vendor remote access accounts when in use. [PCI DSS 8.1.5]

6.7. Account Creation, Deletion, and Removal – The BU shall control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. {PCI DSS 8.1.2]

6.7.1. Account Removal - The BU shall notify account managers within 24 hours when accounts are no longer required; users are separated or transferred; and individual system usage or need-to-know changes. [NIST 800-53 AC-2h] [PCI DSS 8.1.3]

6.7.2. (P) **Immediate Removal of Separated Users** - The BU shall immediately revoke access for any separated users. [PCI DSS 8.1.3]

6.7.3. (P) **Automatic Removal of Temporary Accounts** - The agency system automatically removes or disables temporary and emergency accounts when the accounts have expired, are no longer associated with a user or individual. are in violation of organizational policy, or have been inactive for a BU-defined time. [NIST 800-53 AC-2(2)] [IRS Pub 1075]

6.7.4. (P) **Disable Accounts** - The BU shall ensure the agency system:

- **a.** Automatically disable inactive accounts after BU -defined time period. [NIST 800-53 AC-2(3)] [IRS Pub 1075]
- **b.** (P-PCI) For agency systems containing cardholder data (CHD) the time period must be no more than 90 days. [PCI DSS 8.1.4]
- **c.** Disables accounts of individuals within 24 hours of discovery of BU-defined significant risks (e.g., intention to use authorized access to systems to cause harm). [NIST 800-53 AC-2(13)]

6.7.5. (P) **Inactivity Logout** - The BU shall ensure that users log out when a BU-defined time-period of expected inactivity is exceeded. [NIST 800-53 AC-2(5)]

6.8. **Access Authorization** - The BU shall authorize access to the agency system based on a valid access authorization; intended system usage; and other attributes as required by the organization or associated mission functions. [NIST 800-53 AC-2i] [HIPAA 164.308 (4)(ii)(B) – Addressable] [PCI DSS 7.1, 7.2]

6.8.1. (P) **Default "Deny-All" Setting** - The BU shall ensure the agency system access control system is set to "Deny all" unless specifically allowed. [PCI DSS 7.2.3]

6.8.2. (P) **Restrict Direct Database Access** - The BU shall ensure the agency system authenticates all access to any database containing Confidential information and restricts direct access or queries to databases to database administrators. [PCI DSS 8.7]

6.9. **Accounts Rights Review** - The BU shall review the privileges assigned to accounts to validate the need for such privileges and for compliance with account management requirements annually. The BU shall reassign or remove privileges, if necessary, to correctly reflect BU mission and business needs. [NIST 800-53 AC-6(7)] [HIPAA 164.308 (4)(ii)(C) – Addressable]

6.10. **Reissues Account Credentials** - The BU shall establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group. [NIST 800-53 AC-2k]

6.11. **Align with Termination Process** - The BU shall align the account management processes with personnel termination and transfer processes. [NIST 800-53 AC-2i]

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 8310 Account Management

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.

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**

STATEWIDE POLICY (8320): ACCESS CONTROLS

DOCUMENT NUMBER:	**P8320**
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 define the correct use and management of logical access controls for the protection of agency systems and assets.

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 - 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 - 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 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 BU Director shall:

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

b. Ensure BU compliance with Access Control Policy; and

c. 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 Access Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU ISO shall:

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

b. Ensure the development and implementation of adequate controls enforcing the Access Controls Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of agency systems and assets.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Access Control PSPs; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding correct use and management of logical access controls for the protection of agency systems and assets.

6. STATEWIDE POLICY

6.1 **Access Enforcement** - The BU shall ensure the agency system enforces approved authorizations for logical access to information and system resources in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST 800-53 AC-3] [HIPAA 164.308(a)(3)(ii)(A) - Addressable, 164.308 (a)(4)(ii)(B) & (C) - Addressable]

6.1.1 (P) **Assign Responsibility** - The BU shall assign to an individual or team the security management responsibility of monitoring and controlling all access to Confidential data. [PCI DSS 12.5.5]

6.2 (P) **Develop Access Control Operational Procedures** - The BU shall develop daily operational security procedures for restricting access to sensitive data are documented, in use, and known to all affected parties. [PCI DSS 7.3]

6.3 (P) **Information Flow Enforcement** - The BU shall ensure the agency system enforces approved authorizations for controlling the flow of information within the system and between connected systems based on BU-defined information flow control policies, including STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections. These policies prohibit direct public access between the Internet and any system component in the Protected agency system. [NIST 800-53 AC-4] [IRS Pub 1075] [PCI DSS 1.3]

6.3.1 (P) **Perimeter Firewalls for Wireless Networks** - The BU shall install perimeter firewalls between any wireless network and the Protected agency system, and configures these firewalls to deny, or control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment into the Protected agency system. [PCI DSS 1.2.3]

6.3.2 (P) **Personal Firewalls** - The BU shall require personal firewall software or equivalent functionality on any portable computing devices (including agency and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the agency network.. [PCI DSS 1.4]

6.4 (P) **Least Privilege** - The BU shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks. [NIST 800-53 AC-6] [IRS Pub 1075] [PCI DSS 7.1]

6.4.1 (P) **Organizational Isolation** - The BU shall implement policies and procedures that protect Confidential information from unauthorized access by other (e.g., larger BU to which the BU is a part of) organizations. [HIPAA 164.308 (a)(4)(ii)(A)]

6.4.1.1 (P) **Shared Host Isolation** – For agencies that provide a shared hosting service to other agencies, the Agency BU shall ensure that agency hosts

are protected from other users and processes on the same host or environment. Specifically, that BU shall ensure that: [PCI DSS A.1]

a. each entity only runs processes that have access to that entity's own environment [PCI DSS A.1.1] and

b. each entity's access and privileges shall be restricted to its own environment. [PCI DSS A.1.2]

6.4.2 (P) **Privileged Accounts** - The BU shall restrict access rights to privileged user accounts to least privileges necessary to perform job responsibilities. [PCI 7.1.1]

6.4.3 (P) **Job Classification** - The BU shall restrict access rights based on individual personnel's job classification and function. [PCI DSS 7.1.3]

6.5 (P) **Authorize Access to Security Functions** - The BU shall explicitly authorize access to the following security functions and security-relevant information: [NIST 800-53 AC-6(1)] [IRS Pub 1075]

a. Establishing system accounts;

b. Configuring access authorizations;

c. Setting events to be audited;

d. Setting intrusion detection parameters;

e. Filtering rules for routers and firewalls;

f. Cryptographic key management information; and

g. Configuration parameters for security services.

6.6 (P) **Non-Privileged Access for Non-Security Functions** - The BU shall require that users of agency system accounts, or roles, with access to security functions (e.g., privileged users), use non-privileged accounts or roles, when accessing non-security functions. [NIST 800-53 AC-6(2)] [IRS Pub 1075]

6.7 (P) **Log Use of Privileged Functions** - The BU shall include execution of privileged functions in the events to be logged by the agency system. [NIST 800-53 AC-6(9)]

6.8 (P) **Prohibit Non-Privileged Users From Executing Privileged Functions** - The BU shall ensure the agency system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. [NIST 800-53 AC-6(10)] [IRS Pub 1075]

6.9 **Unsuccessful Logon Attempts** - The BU shall ensure the agency system enforces a BU specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a BU specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is

exceeded, consistent with the Statewide Access Control Standard 8320. [NIST 800-53 AC-7] [PCI DSS 8.1.6]

6.10 System Use Notification - The BU shall ensure the agency system: [NIST 800-53 AC-8]

6.10.1 Displays to users a BU-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall state the following:

- **a.** Users are accessing an agency system owned by the State of Arizona;
- **b.** Agency system usage may be monitored, recorded, and subject to audit;
- **c.** Unauthorized use of the agency system is prohibited and subject to criminal and civil penalties; and
- **d.** Use of the agency system indicates consents to monitoring and recording.
- **e.** Retains the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the agency system; and
- **f.** For publicly accessible systems; the agency system shall also:
- **g.** Display to users the system use agency information before granting further access;
- **h.** Display to users references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- **i.** Include in the notice given to public users of the agency system, a description of the authorized uses of the system.

6.11 (P) **Session Lock** - The BU shall ensure the agency system prevents further access to the system by initiating a BU specified limit of time inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures. If the user does not reestablish access within a BU specified limit of time the session is dropped. [NIST 800-53 AC-11] [IRS Pub 1075] [HIPAA 164.312 (a)(2)(iii)] [PCI DSS 8.1.7, 8.1.8]

6.11.1 (P) **Pattern-Hiding Display -** The BU shall ensure that the system conceals, via the device lock, information previously visible on the display with a publicly viewable image. [NIST 800-53 AC-11(1)]

6.11.2 (P) Session Termination - The BU shall ensure that the system automatically terminates a user session after BU-defined conditions or trigger events. [NIST 800-53 AC-12]

6.12 Permitted Actions Without Identification or Authentication - The BU shall identify user actions that can be performed on the agency system without identification or authentication consistent with BU missions; and documents and provides support rationale in the security plan for the agency system, user actions not requiring identification or authentication. [NIST 800-53 AC-14]

6.13 Remote Access - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the agency system prior to allowing such connections. [NIST 800-53 AC-17]

6.14 (P) **Automated Monitoring / Control** - The BU shall ensure the agency system employs automated mechanisms to monitor and control remote access methods (e.g., detection of cyber-attacks such as false logins, denial of service-attacks, and compliance with remote access policies such as strength of encryption). [NIST 800-53 AC-17(1)] [IRS Pub 1075]

6.14.1 (P) **Security Using Encryption** - The BU shall ensure the agency system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-17(2)] [IRS Pub 1075] [PCI DSS 2.3, 4.1]

6.14.2 (P) **Managed Access Control Points** - The BU shall ensure the agency system routes all remote accesses through authorized and managed network access control points. [NIST 800-53 AC-17(3)] [IRS Pub 1075]

6.14.3 (P) **Privileged Access Commands** - The BU shall authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence, for BU-defined needs, and documents the rationale for such access in the security plan for the agency system. [NIST 800-53 AC-17(4)] [IRS Pub 1075]

6.15 Wireless Access - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and authorizes wireless access to the agency system prior to allowing such connections that are consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-18]

6.15.1 (P) **Wireless Authentication and Encryption** - The BU shall ensure the agency system protects wireless access to the agency system using authentication of users and devices and encryption. [NIST 800-53 AC-18(1)] [IRS Pub 1075] [PCI DSS 4.1]

6.15.2 Wireless Encryption Strength – The BU shall ensure wireless networks transmitting Confidential data use industry best practices to implement strong encryption for authentication and transmission. [PCI DSS 4.1.1]

6.15.3 (P) **Disable Wireless Networking** - The BU shall disable, when not in use, wireless networking capabilities embedded within system components prior to issuance and deployment. [NIST 800-53 AC-18(3)]

6.16 Access Control for Mobile Devices - The BU shall establish configuration guidance, connection requirements, and implementation guidance for BU controlled mobile devices to include when such devices are outside of controlled areas; and authorizes connection of mobile devices to agency systems. [NIST 800-53 AC-19]

6.16.1 (P) **Full Device Encryption** - The BU shall employ full-device or container-based encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to agency systems or to create, transmit or process Confidential information. [NIST 800-53 AC-19(5)] [IRS Pub 1075] [HIPAA 164.308 (e)(2)(ii) - Addressable] [PCI DSS 4.1]

6.16.2 (P) **Purge or Wipe Mobile Device** - The BU shall ensure that information on mobile devices are purged or wiped from mobile devices enabled for use with agency systems based on sanitization techniques using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250 after a BU-defined number of consecutive invalid logon attempts. [NIST 800-53 AC-7(2)]

6.17 Use of External Systems - The BU shall: [NIST 800-53 AC-20]

- **a.** Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to access the system from external systems; and process, store, or transmit (Agency) BU controlled information using external systems. or
- **b.** Prohibit the use of BU-defined types of external systems.

6.17.1 (P) **Limits on Authorized Use** - The BU shall permit authorized individuals to use an external system to access the agency system to process, store, or transmit BU controlled information only after: [NIST 800-53 AC-20(1)] [IRS Pub 1075]

- **a.** Verification of the implementation of controls on the external system as specified in the BU's information security and privacy policies and security and privacy plans; or
- **b.** Retention of approved system connection or processing agreements with the organizational entity hosting the external system in accordance with the Arizona State Library Records Retention Schedule,

Management Records, Item 6: http://apps.azlibrary.gov/records/general_rs/Management.pdf.

6.17.2 (P) **Portable Storage Devices** - The BU shall restrict or prohibit the use of BU controlled portable storage devices by authorized individuals on external systems using BU defined restrictions. [NIST 800-53 AC-20(2)] [IRS Pub 1075]

6.17.3 (P) **Restricted Use of Non-BU Owned Systems** - The BU shall restrict the use of BU owned systems or system components to process, store, or transmit organizational information using BU-defined restrictions [NIST 800-53 AC-20(3)].

6.18 (P) **Information Sharing** - The BU shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access and use restrictions for BU-defined circumstances; and shall employ BU defined mechanisms or processes to assist users in making information sharing and collaboration decisions. [NIST 800-53 AC-21] [IRS Pub 1075] [PCI DSS 12.8]

6.18.1 (P) **Maintain List of Service Providers** - The BU shall maintain a list of service providers, including a description of the service provided, that have access to Confidential data. [PCI DSS 12.8.1]

6.18.2 (P) **Written Agreements** - The BU shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of Confidential data the service providers possess. [PCI DSS 12.8.2]

6.18.3 (P) **Due Diligence** - The BU shall ensure there is an established process for engaging service providers including proper due diligence prior to engagement. [PCI DSS 12.8.3]

6.18.4 (P) **Service Provider Monitoring Program** - The BU shall maintain a program to monitor service provider's compliance with requirements for the protection of Confidential data. [PCI DSS 12.8.4]

6.18.5 **(P) Service Provider Information** - The BU shall maintain information about which information security requirements are managed by each service provider, and which are managed by the BU. [PCI DSS 12.8.5]

6.19 **Publicly Accessible Content** - The BU shall: [NIST 800-53 AC-22]

a. Designate individuals authorized to make information publicly accessible system;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible agency system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible agency system for nonpublic information annually and remove such information, if discovered.

7. DEFINITIONS AND ABBREVIATIONS

1.1 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 8320 Access Controls

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections

8.4 Statewide Standard 8320, Access Control

8.5 Statewide Standard 8350, System Communication and Protection

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

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

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

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

8.10 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number GS 1005, Arizona State Library, Archives and Public Records, Item Number 6

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**

	STATEWIDE # POLICY	**State of Arizona**

STATEWIDE POLICY (8330): SYSTEM SECURITY AUDIT

DOCUMENT NUMBER:	**P8330**
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 protect agency systems and data by ensuring the Budget Unit (BU) and agency systems have the appropriate controls and configurations to support audit log generation, protection, and review.

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 - 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 - 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 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 BU Director shall:

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

b. Ensure BU compliance with System Security Audit Policy; and

c. 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 System Security Audit Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU ISO shall:

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

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

c. Ensure all personnel understand their responsibilities with respect to the generation, protection and review of audit logs.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on System Security Audit Policies; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding the generation, protection and review of audit logs.

6. STATEWIDE POLICY

6.1 Event Logging -The BU shall: [NIST 800-53 AU-2]

- **a.** Identify the types of events the agency system is capable of logging in support of the audit function. .
- **b.** Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection of criteria for events to be logged;
- **c.** Specify the event types for logging within the system as defined in the Statewide System Security Audit Standard S8330 along with the frequency of logging for each identified event type;
- **d.** Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents;
- **e.** Ensure the events listed in the Statewide System Security Audit Standard S8330 are logged within the agency system
- **f.** Review and update the event types selected for logging annually; and [IRS Pub 1075]
- **g.** (P) For agencies that provide a shared hosting service to other agencies, ensure that logging and audit trails are unique to each agencies environment. [PCI DSS A.1.3]

6.1.1 Content of Audit Records - The BU shall ensure the agency systeminformation system generates audit records containing information that establishes: [NIST 800-53 AU-3] [PCI DSS 10.3]

- **a.** What type of event occurred; [PCI DSS 10.3.2] [IRS Pub 1075]
- **b.** When the event occurred; [PCI DSS 10.3.3] [IRS Pub 1075]
- **c.** Where the event occurred; [PCI DSS 10.3.5] [IRS Pub 1075]
- **d.** The source of the event (i.e., name of the affected data, system component, or resource); [PCI DSS 10.3.6] [IRS Pub 1075]
- **e.** The outcome of the event; and [PCI DSS 10.3.5]
- **f.** The identity of any individuals, or subjects or objects/entities associated with the event. [PCI DSS 10.3.1] [IRS Pub 1075]

6.1.2 (P) **Additional Audit Information** - The BU shall ensure the state systeminformation system generates audit records containing BU-defined additional information. [NIST 800-53 AU-3(1)] [IRS Pub 1075]**(P) Audit Reviews and Updates** - The BU shall review

and update the selected audited events annually, or as required. [NIST 800-53 AU-2(3)] [IRS Pub 1075]

6.1.3 Limit Personally Identifiable Information Elements - The BU shall limit personally identifiable information contained in audit records to the BU-defined elements identified in the privacy risk assessment. [NIST 800-53 AU-3(3)

6.2 Audit Storage Capacity - The BU shall allocate audit log storage capacity to accomodate BU-defined audit log storage requirements. [NIST 800-53 AU-4]

6.3 Response to Audit Processing Failures - The BU shall ensure the agency system alerts BU-defined personnel or roles in the event of an audit logging process failure; and shuts down the agency system, overwrites the oldest audit records, or stops generating audit records. [NIST 800-53 AU-5]

6.3.1 (P) **Storage Capacity Warning** - The BU shall ensure the agency system provides a warning to BUI-defined personnel when allocated audit log storage volume reaches a maximum capacity. [NIST 800-53 AU-5(1)] [IRS Pub 1075]

6.4 Audit Review, Analysis, and Reporting - The BU shall: [NIST 800-53 AU-6] [HIPAA 164.308 (a)(1)(ii)(D)] [HIPAA 164.312 (b)]

- **a.** eview and analyze agency system audit records periodically for indications of inappropriate or unusual activity and the potential impact;
- **b.** Report findings to BU-defined personnel or roles; and
- **c.** Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
- **d.** (P-PCI) Agency systems with cardholder data (CHD) shall perform this review daily. [PCI DSS 10.6, 10.6.1, 10.6.2, 10.6.3]

6.4.1 (P) **Process Integration** - The BU shall integrate audit record review, analysis, and reporting processes using automated mechanisms. [NIST 800-53 AU-6(1)] [IRS Pub 1075]

6.4.2 (P) **Correlate Audit Repositories** - The BU shall analyze and correlate audit records across different repositories to gain BU-wide situational awareness. [NIST 800-53 AU-6(3)] [IRS Pub 1075]

6.5 Audit Reduction and Report Generation - The BU shall ensure the agency system provides and implements an audit reduction and report generation capability that

supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and does not alter original content or time ordering of audit records. [NIST 800-53 AU-7]

6.5.1 (P) **Automatic Processing** - The BU shall ensure the agency system provides and implements the capability to process, sort, and search audit records for events of interest based on the following audit fields within audit records: [NIST 800-53 AU-7(1)] [IRS Pub 1075]

- **a.** Individual identities
- **b.** Event types
- **c.** Event locations
- **d.** Event times and time frames
- **e.** Event dates
- **f.** System resources involved, IP addresses involved
- **g.** Information object accessed

6.6 Time Stamps - The BU shall ensure the agency system uses internal system clocks to generate timestamps for audit records; and records time stamps for audit records that meet the BU-defined granularity of time measurement and that can use Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or have a fixed local time offset from UTC or GMT, or that include the local time offset as part of the time stamp. [NIST 800-53 AU-8]

6.6.1 (P) **Synchronization with Authoritative Time Source** - The BU shall ensure the agency system compares the internal agency system clocks a BU-defined frequency with a BU-defined time source and synchronizes the internal agency system clocks to the authoritative time source when the time difference is greater than a BU-defined time period. [NIST 800-53 SC-45(1)] [PCI DSS 10.4, 10.4.1, 10.4.3]

6.6.2 (P) **Protection of Time Data** - The BU shall ensure the agency system protects time-synchronization settings by restricting access to such settings to authorized personnel and logging, monitoring, and reviewing changes. [PCI DSS 10.4.2]

6.7 Protection of Audit Information - The BU shall ensure the agency system protects audit information and audit logging tools from unauthorized access, modification, and deletion; and alerts BU-defined personnel upon detection of unauthorized access, modification, or deletion of audit information. [NIST 800-53 AU-9] [PCI DSS 10.5] [IRS Pub 1075]

6.7.1 (P) **Access by Subset of Privileged Users** -The BU shall authorize access and modification to management of audit logging functionality to only a BU-defined subset of privileged users. [NIST 800-53 AU-9(4)] [IRS Pub 1075] [PCI DSS 10.5.1, 10.5.2]

6.7.2 (P) **Audit Trail Backup** - The BU shall promptly back up audit trail files to a centralized log server or media that is difficult to alter. [PCI DSS 10.5.3]

6.7.3 (P) **Audit Backup on Separate Physical Systems** - The BU shall ensure the agency system backs up audit records onto a physically different system or system components than the system or component being audited. [PCI DSS 10.5.4]

6.7.4 (P) **File Integrity Monitoring of Audit Logs** - The BU shall ensure the agency system uses file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts. [PCI DSS 10.5.5]

6.8 Audit Record Retention - The BU shall retain audit records for a BU-defined time period consistent with the records retention policy with a BU-defined time period available for immediate analysis to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. For agency systems with cardholder data these defined times are at least one year with a minimum of three months immediately available for analysis. [NIST 800-53 AU-11] [PCI DSS 10.7]

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:
http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf
Item 16.b.

6.9 Audit Generation - The BU shall ensure the agency system: [NIST 800-53 AU-12]

a. Provides audit record generation capability for the event types, defined in Section 6.1.a (Event Loggins), at servers, firewalls, workstations, mobile devices, and other BU-defined system components and services;

b. (P) Anti-virus programs are generating audit logs; [PCI DSS 5.2]

c. Allows BU-defined personnel or roles to select the event types that are to be logged by specific components of the agency system; and

d. Generates audit records for the event types, defined in Section 6.1.c (Event Loggings), with the content defined in Section 6.2 (Content of Audit Records).

6.10 (P) **Cross Agency Auditing** - The BU shall employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across BU boundaries. Note: This requirement applies to outsourced data centers and cloud service providers. The provider must be held accountable to protect and share audit information with the BU through the contract. [NIST 800 53 AU-16]

6.11 (P) **Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for monitoring all access to network resources and Confidential data are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 10.9]

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 8330 SYSTEM SECURITY AUDIT

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, Information Technology (IT) Records, Schedule Number: 000-12-41, Arizona State Library, Archives and Public Records, Item Number 16b

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

	STATEWIDE # POLICY	**State of Arizona**

STATEWIDE POLICY (8340): IDENTIFICATION AND AUTHENTICATION

DOCUMENT NUMBER:	**P8340**
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 define the security requirements for establishing and maintaining user accounts for 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 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 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 BU Director shall:

- **a.** Be responsible for the correct and thorough completion of Agency Information Security PSPs within the BU;
- **b.** Ensure BU compliance with Identification and Authentication Policy; and
- **c.** 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 Identification and Authentication Policy is periodically reviewed and updated to reflect changes in requirements

5.6 BU ISO shall:

- **a.** Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU Information Security PSPs;
- **b.** Ensure the development and implementation of adequate controls enforcing the Identification and Authentication Policy for the BU; and
- **c.** Ensure all personnel understand their responsibilities with respect to establishing and maintaining user accounts for agency systems.

5.7 Supervisors of agency employees and contractors shall:

- **a.** Ensure users are appropriately trained and educated on Identification and Authentication Policies; and
- **b.** Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

- **a.** Become familiar with this policy and related PSPs; and
- **b.** Adhere to PSPs regarding the establishment and maintenance of user accounts for agency systems.

6. STATEWIDE POLICY

6.1.1 **Identification and Authentication of Organizational Users** - The BU shall ensure the agency system **uniquely** identifies and authenticates organizational users and associate that unique identification with processes acting on behalf of those users. [NIST 800 53 IA-2] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]

6.1.2 **Access to Privileged Accounts** - The BU shall ensure the agency system implements multifactor authentication for access to privileged accounts. [NIST 800 53 IA-2(1)] [IRS Pub 1075]

6.1.3 **Access to Non-Privileged Accounts** - The BU shall ensure the agency system implements multifactor authentication for access to non-privileged accounts. [NIST 800 53 IA-2(2)] [IRS Pub 1075]

6.1.4 (P) **Network Access to Privileged Accounts – Replay Resistant** - The BU shall ensure the agency system implements replay-resistant authentication mechanisms for access to privileged accounts. [NIST 800 53 IA-2(8)]

6.1.5 **Access to Accounts (Privileged and Non-Privileged) – Separate Device** - The BU shall ensure the agency system implements multifactor authentication for remote access to organizational accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets statewide cryptographic standards for strength of mechanism. [NIST 800 53 IA-2(6)] [PCI DSS 8.3, 8.3.1] [IRS Pub 1075]

6.2 (P) **Device Identification and Authentication** - The BU shall ensure the agency system uniquely identifies and authenticates before establishing a local, remote, or network connection. [NIST 800 53 IA-3] [IRS Pub 1075] [HIPAA 164.312 (d)]

6.3 **Identifier Management** - The BU shall manage the agency system identifiers by: [NIST 800 53 IA-4] [PCI DSS 8.5]

- **a.** (P) Ensuring that group, shared, or generic account identifiers and authentication methods are not used; [PCI DSS 8.5, 8.6]
- **b.** Receiving authorization from BU-defined personnel or roles to assign individual, role, service, or device identifier;
- **c.** Selecting an identifier that identifies an individual, role, service, or device;
- **d.** Assigning the identifier to the intended individual, role, service, or device;
- **e.** Preventing reuse of identifiers for one year; and
- **f.** Disabling the identifier after 90 days of inactivity. [PCI DSS 8.1.4]

6.3.1 **Identify User Status** - The BU shall manage individual identifiers by uniquely identifying each individual with a BU-defined dynamic identifier policy. [NIST 800 53 IA-4(4)]

6.4 Authenticator Management - The BU shall manage the agency system authenticators (e.g., passwords, tokens, certificate, and key cards) by: [NIST 800 53 IA-5] [HIPAA 164.308(a)(5)ii)(D)] [HIPAA 164.308 (d)]

- **a.** Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; [PCI DSS 8.2.2]
- **b.** Establishing initial authenticator content for authenticators issued by the BU;
- **c.** Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- **d.** Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- **e.** Changing default content of authenticators prior to first use;
- **f.** Changing or refreshing authenticators BU-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI certificates, and key cards)or when a suspected compromise occurs;
- **g.** Protecting authenticator content from unauthorized disclosure and modification;
- **h.** Requiring individuals to take, and having devices implement, specific controls to protect authenticators; [PCI DSS 8.6]
- **i.** Changing authenticators for group or role accounts when membership to those accounts changes; and
- **j.** Employing at least one of the following methods to authenticate all users: [PCI DSS 8.2]
    1. Password-Based Authentication
    2. PKI-based Authentication
    3. In Person or Trusted Third Party Registration
    4. Hardware Token-based Authentication

6.4.1 **Password-Based Authentication** - The BU shall ensure the agency system, for password-based authentication enforces password controls consistent with the

Statewide Standard 8340, Identification and Authentication. [NIST 800 53 IA-5(1)] [PCI DSS 8.2.3, 8.2.4, 8.2.5, 8.2.6]

a. **Password Encryption -** The BU shall ensure the use of strong cryptography and render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. [PCI DSS 8.2.1]

6.4.2 (P) **Public Key-based Authentication** - The BU shall ensure the agency system, for Public Key-based authentication: [NIST 800 53 IA-5(2)] [IRS Pub 1075]

a. For public key-based authentication:

1. Enforces authorized access to the corresponding private key;

2. Maps the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

2. Implements a local cache of revocation data to support path discovery and validation.

6.4.3 Protection of Authenticators - The BU shall protect authenticators commensurate with the security category of the information to which use of the authenticator permits access. [NIST 800 53 IA-5(6)]

6.5 **Authenticator Feedback** - The BU shall ensure the agency system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals. [NIST 800 53 IA-6]

6.6 **Cryptographic Module Authentication** - The BU shall ensure the agency system implements mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. [NIST 800 53 IA-7]

6.7 **Identification and Authentication (Non-Organizational Users)** - The BU shall ensure the agency system uniquely identifies and authenticates non-organizational users or processes acting on behalf of non-organizational users. [NIST 800 53 IA-8] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]

6.7.1 **Acceptance of External Authenticators** - The BU shall ensure the agency system accepts only external authenticators that are NIST-compliant; and

document and maintain a list of accepted external authenticators. [NIST 800 53 IA-8(2)]

6.7.2 **Use of Defined Profiles** - The BU shall ensure the agency system information system conforms to the BU-defined identity management profiles. [NIST 800 53 IA-8(4)]

6.8 **Re-Authentication** - The BU shall ensure the agency system requires users to re-authenticate when the following circumstances or situations requiring re-authentication occur: [NIST 800 53 IA-11]

a. change in role, authenticators, or credentials;

b. execution of BU-defined privileged functions; or

c. after a BU-defined period of time.

6.9 (P) **Identity Proofing** - The BU shall identity proof (the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system) users that require accounts for logical access to agency systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; resolve user identities to a unique individual; and collect, validate, and verify identity evidence. [NIST 800 53 IA-12]

6.9.1 **(P) Identity Evidence** - The BU shall require evidence of individual identification be presented to the registration authority. [NIST 800 53 IA-12(2)]

6.9.2 **(P) Identity Evidence Validation and Verification** - The BU shall require that the presented identity evidence be validated and verified through BU-defined methods of validation and verification. [NIST 800 53 IA-12(3)]

6.9.3 **(P) Address Confirmation** - The BU shall require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital) of record. [NIST 800 53 IA-12(5)]

6.10 (P) **Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 8.4, 8.8]

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

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 8340 IDENTIFICATION AND AUTHENTICATION

8.2 Statewide Policy Exception Procedure

8.3 Statewide Standard 8340, Identification and Authentication

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

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

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

8.7 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

	STATEWIDE # POLICY	**State of Arizona**

STATEWIDE POLICY (8350): SYSTEM AND COMMUNICATION PROTECTIONS

DOCUMENT NUMBER:	**P8350**
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 establish the baseline controls for the protection of agency systems and their communications.

3. SCOPE

3.1 Application to Budget Units (BU) - 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 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 State CIO 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 BU Director shall:

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

b. Ensure BU compliance with System and Communication Protections Policy; and

c. 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 System and Communication Protections Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU ISO shall:

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

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

c. Ensure all personnel understand their responsibilities with respect to the protection of agency systems and their communications.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on System and Communication Protections Policies; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding the establishment and maintenance of user accounts for agency systems.

6. (AGENCY) POLICY

6.1 Network and Architectural Controls - The BU shall ensure the agency system implements the following network and network architectural controls.

6.1.1 (P) **Application Partitioning** - The BU shall ensure the agency system separates user functionality, including user interface services, either physically or logically from agency system management functionality (e.g., privileged access). [NIST 800 53 SC-2] [IRS Pub 1075]

6.1.2 **Boundary Protection** - The BU shall ensure the agency 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 subnetworks 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.

6.1.3 **(P) Implement DMZ (demilitarized zone) - The BU shall ensure the agency** system **prohibits direct public access between the Internet and any system component in the Protected agency** system**. The DMZ: [PCI DSS 1.3]**

- **a.** Limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [PCI DSS 1.3.1]
- **b.** Limits inbound Internet traffic to IP addresses within the DMZ; [PCI DSS 1.3.2]
- **c.** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [PCI DSS 1.3.3]
- **d.** Does not allow unauthorized outbound traffic from the Protected agency system to the Internet; [PCI DSS 1.3.4]
- **e.** Permits only “established” connections into the network. [PCI DSS 1.3.5]
- **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 [PCI DSS 1.3.6]
- **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). [PCI DSS 1.3.7]

6.1.3.1 (P) **Firewall Configuration Standards** - The BU shall establish and implement firewall and router configuration standards that include the following: [PCI DSS 1.1]

- **a.** A formal process for approving and testing all network connections and changes to the firewall and router configurations; [PCI DSS 1.1.1]
- **b.** Current network diagrams that identifies all connections between the agency system and other networks, including any wireless networks; [PCI DSS 1.1.2]
- **c.** Current diagram that shows all Confidential data flows across systems and networks; [PCI DSS 1.1.3]
- **d.** Requirements for a firewall at each Internet connection and between any DMZ and the Internal network zone; [PCI DSS 1.1.4]
- **e.** Description of groups, roles, and responsibilities for management of network components; [PCI DSS 1.1.5]
- **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 nonsecure. [PCI DSS.1.1.6]
- **g.** Requirement to review firewall and router rule sets at least every six (6) months. [PCI DSS 1.1.7]

6.1.3.2 (P) **Firewall Configuration** - The BU shall build firewall and router configurations that restrict access points between Non-Protected systems (Standard agency systems or untrusted networks) and any system components in the Protected agency system. The configurations: [PCI DSS 1.2]

- **a.** Restrict inbound and outbound traffic to that which is necessary for the Protected agency system; [PCI DSS 1.2.1]
- **b.** Secure and synchronize router configuration files; and [PCI DSS 1.2.2]
- **c.** Implement perimeter firewalls between all wireless networks and the Protected agency 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 agency system. [PCI DSS 1.2.3]

6.1.4 (P) **Limit Access Points** - The BU shall limit the number of external network connections to the agency system. [NIST 800 53 SC-7(3)] [IRS Pub 1075]

6.1.5 (P) **Deny by Default / Allow by Exception** - The BU shall ensure the agency 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)] [IRS Pub 1075]

6.1.6 (P) **Network Disconnect** - The BU shall ensure the agency 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] [IRS Pub 1075]

6.2 Server Controls - The BU shall ensure the agency system implements the following controls for servers and components of the agency system:

6.2.1 (P) **Information in Shared Resources** - The BU shall ensure the agency system prevents unauthorized and unintended information transfer using shared system resources. [NIST 800 53 SC-4] [IRS Pub 1075]

6.2.2 (P) **Prevent Split Tunneling for Remote Devices** - The BU shall ensure the agency 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)] [IRS Pub 1075]

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

6.2.4 (P-PII) Personally Identifiable Information - The BU shall ensure that agency systems that process personally identifiable information: [NIST 800 53 SC-7(24)]

- **a.** Applies BU-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.

6.2.5 (P) **Single Primary Function (Database)** - The BU shall ensure agency system components (e.g., servers) implementing a database implement only one primary function (the database) on this server. [PCI DSS 2.2.1]

6.2.6 (P-PCI) **Single Primary Function -** For agency systems storing, processing, or transmitting cardholder data (CHD), the BU shall ensure all agency system components (e.g., server) implement only one primary function per server to

prevent functions that require different security levels from coexisting on the same server. [PCI DSS 2.2.1]

6.2.7 (P) **Least Functionality** - The BU 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] [PCI DSS 2.2.2]

a. (P-PCI) - For agency systems with cardholder data (CHD) unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be removed. [PCI DSS 2.2.5]

b. (P) **Otherwise Protected** - For all other agency systems unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be disabled or removed. [PCI DSS 2.2.2, 2.2.4]

c. Implement additional security features for any required services, protocols, or daemons that are considered to be nonsecure. [PCI DSS 2.2.3]

d. (P) **Periodic Review** - The BU 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)]

e. (P) **Prevent Program Execution** - The BU shall ensure that the agency system is configured to prevent program execution in accordance with BU-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)]

f. (P) **Authorized Software - Allow By Exception** - The BU shall identify BU-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)]

6.2.8 (P) **Secure Configuration** - The BU shall configure the agency system component (e.g., server) security parameters to prevent misuse. [PCI DSS 2.2.4]

6.3 Secure Services - The BU shall ensure the agency system implements the following controls for services provided:

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

6.3.2 Cryptographic Services - The BU shall ensure the agency system implements the following cryptographic services:

a. Cryptographic Protection - The agency system shall determine the BU-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] [PCI DSS 4.1] [HIPAA 164.312(a)(2)(iv), (e)(2)(i)]

b. Cryptographic Key Establishment and Management - The BU 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]

6.3.2.1 (P) **Key Protection** - The BU shall protect all keys used to secure Confidential data against disclosure and misuse: [PCI DSS 3.5]

a. Restrict access to cryptographic keys to the fewest number of custodians necessary; and [PCI DSS 3.5.2]

b. Store secret and private keys used to encrypt/decrypt Confidential data in one (or more) of the following forms at all times: [PCI DSS 3.5.3]

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key
- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)
- As at least two full-length key components or key shares, in accordance with an industry accepted method

c. Store cryptographic keys securely in the fewest possible locations. [PCI DSS 3.5.4]

6.3.2.2 (P) **Key Management Process** - The BU shall fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of Confidential data including the following: [PCI DSS 3.6]

a. Generation of strong cryptographic keys; [PCI DSS 3.6.1]

b. Secure cryptographic key distribution; [PCI DSS 3.6.2]

c. Secure cryptographic key storage; [PCI DSS 3.6.3]

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; [PCI DSS 3.6.4]

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; [PCI DSS 3.6.5]

f. If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control; [PCI DSS 3.6.6]

g. Prevention of unauthorized substitution of cryptographic keys; and [PCI DSS 3.6.7]

h. Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. [PCI DSS 3.6.8]

6.3.2.3 (P) **Public Key Infrastructure Certificates** -The BU 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] [IRS Pub 1075]

6.3.3 (P) **External Telecommunications Services** - The BU shall ensure: [NIST 800 53 SC-7(4)] [IRS Pub 1075]

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 or business need and duration of that need;

e. Review exceptions to the traffic flow policy annually and remove exceptions that are no longer supported by an explicit mission or business need;

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

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

6.3.4 (P) **Transmission Confidentiality and Integrity** - The BU shall ensure the agency system protects the confidentiality and, if required, integrity of transmitted information. [NIST 800 53 SC-8] [IRS Pub 1075] [HIPAA 164.312(c)(1), (c)(2), (e)(1)]

6.3.4.1 (P) Cryptographic or Alternate Physical Protection - The BU shall ensure the agency system prevents unauthorized disclosure of information and detects changes to information during transmission. [NIST 800 53 SC-8(1)] [IRS Pub 1075] [HIPAA 164.312(c)(1), (c)(2), (e)(1)]

6.3.5 (P) **Mobile Code** - The BU shall: [NIST 800 53 SC-18] [IRS Pub 1075]

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 the agency system.

6.3.6 **Collaborative Computing Devices** - The BU shall ensure the agency 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]

6.3.7 (P) **Session Authenticity** - The BU shall ensure the agency 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] [IRS Pub 1075]

6.3.8 **Secure Name/Address Resolution Service** - The BU shall ensure the agency system implements the following with respect to secure name/ address resolution service:

a. Secure Name/Address Resolution Service (Authoritative Service) - The BU shall ensure the agency system provides additional data origin authentication 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) - The BU shall ensure the agency 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 - The BU shall ensure the agency systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation. [NIST 800 53 SC-22]

6.3.9 (P) **Protection of Information at Rest** - The BU shall ensure the agency system protects the confidentiality and integrity of BU-defined data at rest. [NIST 800 53 SC-28]

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

b. (P-FTI) **Protection of Taxpayer Information at Rest** - For systems with taxpayer information, The BU shall ensure the agency system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of taxpayer information at rest. [IRS Pub 1075]

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

6.4 Establish Operational Procedures – The BU 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. [PCI DSS 1.5, 2.5, 3.7, 4.3]

6.5 Change Vendor Defaults – The BU 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.). [PCI DSS 2.1]

6.5.1 Change Wireless Vendor Defaults - For wireless environments connected to the agency system or transmitting Confidential data change wireless vendor defaults,

including but not limited to default wireless encryption keys, passwords, and SNMP community strings. [PCI DSS 2.1.1]

6.6 Configuration Standards – The BU shall ensure that configuration standards for all system components are developed. The BU 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: [PCI DSS 2.2]

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)

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 8350 SYSTEM AND COMMUNICATIONS PROTECTION

8.2 Statewide Standard 8350, System and Communication Protection

8.3 Statewide Policy Exception Procedure

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

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

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

8.7 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

9. 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**

STATEWIDE POLICY (8410): SYSTEM PRIVACY

DOCUMENT NUMBER:	**(P8410)**
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 standard is to provide more detailed guidance for the development of a system privacy notice based on standards, regulations, and best practices.

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.a 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.b 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 all (Agency) BU activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

b. Review and approve or disapprove all BU security and privacy PSPs and exceptions to existing PSPs; and

c. Identify and convey to the State CIO the risk to Confidential data based on current implementation of privacy controls and mitigation options to improve privacy.

5.3 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security PSPs.

5.4 State Chief Privacy Officer (CPO) shall:

a. Advise the State CIO and State CISO on the completeness and adequacy of the BU activities and documentation for data privacy provided to ensure compliance with statewide privacy PSPs throughout all state BUs;

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

c. Identify and convey, to the State CIO and State CISO, the privacy risk to state systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.5 BU Director shall:

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

b. Ensure compliance with BU PSPs; and

c. Promote efforts within the BU to establish and maintain effective privacy controls on BU systems and premises.

5.6 BU CIO shall:

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

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

5.7 BU ISO shall:

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

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

c. Support the agency privacy officers and provide them with adequate information;

d. Request changes and/or exceptions to existing PSPs from the State CISO; and

e. Ensure all personnel understand their responsibilities with respect to privacy of Confidential data.

5.8 The BU Privacy Officer shall:

a. Advise the State CISO and the State CPO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with privacy laws, regulations, statutes and statewide privacy PSPs throughout all agency BUs; and

b. Assist the agency to ensure the privacy of sensitive personal information within the agency's possession.

c. Reviews and approves BU privacy PSPs and requested exceptions from the statewide privacy PSPs; and

d. Identify and convey to the BU CIO the privacy risk to agency systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.9 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.

5.10 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding system privacy.

6. (AGENCY) POLICY

6.1 (P) **Policy and Procedures** - The BU shall [NIST 800 53 PT-1]

a. Develop, document, and disseminate to BU-defined roles

1. A BU-level PII processing and transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the PII processing and transparency policy and the associated PII processing and transparency controls;

b. Designate a BU-defined official to manage the development, documentation, and dissemination of the PII processing and transparency policy and procedures; and

c. Review and update the current PII processing and transparency:

1. Policy annually and following data breach events; and

2. Procedures annually and following data breach events or changes in operations to necessitate procedural changes.

6.2 (P) **Authority to Collect** - The BU shall determine and document the laws, executive orders, directive, regulations, or policies that permit the processing and processing operations (e.g., creation, collection, use, processing, maintenance, dissemination, disclosure, logging, generation, transformation, analysis, and disposal) of PII and restricts processing and processing operations to only that which is authorized. . For additional specificity on the authority to collect, refer to Standard 8330, System Security Audit. [NIST 800 53 PT-2] [Privacy Acts] [HIPAA 164.520(a)(1)]

6.3 (P) **Purpose Specification** - The BU shall:[NIST 800 53 PT-3] [HIPAA 164.520(a)(1)] [ARS 41-4152]

a. Identify and document the purpose(s) for processing personally identifiable information (PII);.

b. Describe the purpose(s) in the public privacy notices and policies of the BU;

c. Restrict the BU-defined processing of PII data to only that which is compatible with the identified purpose(s); and

d. Monitor changes in processing PII and implement training, monitoring, and/or auditing mechanisms to ensure that any changes are made in accordance with BU-defined requirements.

6.4 (P) **Privacy Program Plan** - The BU shall: [NIST 800 53 PM-18]

a. Develop and disseminate a BU-wide privacy program plan that provides an overview of the BU's privacy program, and;

3. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program;

4. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;

5. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities;
6. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program;
7. Reflects coordination among organizational entities responsible for the different aspects of privacy; and
8. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the state; and

b. Update the plan annually and to address changes in privacy laws and policy and BU-changes and problems identified during plan implementation or privacy control assessments.

6.5 (P) **Privacy Program Leadership Role** - The BU shall appoint a senior agency official for privacy with the **authority**, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the BU-wide privacy program. [NIST 800 53 PM-19] [HIPAA 164.530(a)(1)] [EO 2008-10]

6.6 (P) **Privacy Reporting** - The BU shall: [NIST 800 53 PM-27]

a. Develop state privacy officer defined privacy reports and disseminate to the State Privacy Officer (SPO) and other appropriate oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and to to senior management and other personnel with responsibility for monitoring privacy program compliance; and

b. Review and update privacy reports as necessary, but at least every three years.]

(P) **Accounting of Disclosures** - The BU, consistent with state privacy acts and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 PM-21] [HIPAA 164.528(a)]

a. Develop and maintain an accurate accounting of disclosures of PII held in each system of records under its control, including:

1. Date, nature, and purpose of each disclosure of a record
2. Name and address of the person or other contact information of the individual or agency to which the disclosure was made; and

b. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer or as required by law. 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: **http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf** Item 10a. and b.; and

c. Make the accounting of disclosures available to the individual to whom the PII relates upon request.

6.7 (P) **Personally Identifiable Information Quality Operations** - The BU shall check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle annually and correct or delete inaccurate or outdated personally identifiable information. [NIST 800-53 SI-18]

a. (P) Individual Requests - The BU shall correct or delete personally identifiable information upon request by individuals or their designated representatives.[NIST 800-53 SI-18(4)]

b. (P) De-identification - The BU shall remove the BU-defined elements of personally identifiable information from datasets and evaluate annually for effectiveness of de-identification. [NIST 800-53 SI-19]

c. (P) Notice of Correction or Deletion - The BU shall notify BU-defined recipients of PII and individuals that the PII has been corrected or deleted. [NIST 800-53 SI-18(5)]

6.7.a (P) **Personally Identifiable Information Quality Management -** The BU shall develop and document BU-wide policies and procedures for: [NIST 800 53 PM-22] [HIPAA 164.526(a)-(f)

a. Reviewing for the accuracy, relevance, timeliness, and completeness of PII across the information life cycle;

b. Correcting or deleting inaccurate or outdated PII;

c. Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and

d. Appeals of adverse decisions on correction or deletion requests.

6.7.b (P) **Minimization of Personally Identifiable Information Used in Testing, Training, and Research** - The BU shall: [NIST 800 53 PM-25]

a. Develop, document, and implement policies and procedures that address the sue of PII for internal testing, training, and research:

b. Limit or minimize the amount of PII used for internal testing, training, and research;Authorize the use of PII when such information is required for internal testing, training, and research; and

6.7.c Review and update policies and procedures annually.(P) **Consent** - The BU shall implement State Privacy Officer (SPO) approved tools and mechanisms for individuals consent to the processing of their PII prior to its collection that facilitate individuals' informed decision-making. [NIST 800 53 PT-4]

6.7.d For collection, use, and disclosures of PII not already authorized by law the BU shall provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection; [HIPAA 164.522(a)(1)]

a. .

6.8 Dissemination of Privacy Program Information - The BU shall maintain a central resource webpage on the BU's principal public website that serves as a central source of information about the BU's privacy program and that: [NIST 800 53 PM-20][HIPAA 164.524(a)]

a. Ensures that the public has access to information about BU privacy activities and can communicate with its senior agency official for privacy;

b. Ensures that organizational privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

d. Publish rules and regulations governing how individuals may request access to records maintained in a system of records; and [HIPAA 164.524(b),(c),(d)]

e. Adhere to requirements and policies and guidance for the proper processing of PII requests. [HIPAA 164.524(b),(c),(d)]

6.8.a Privacy Notice - The BU shall provide notice to individuals about the processing of PII that: [NIST 800 53 PT-5][HIPAA 164.520(c)] [ARS 41-4152]

a. Is available to individuals upon first interacting with an organization, and subsequently at BU-defined frequency;

b. Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language;

c. Identifies the authority that authorizes the processing of personally identifiable information;

d. Identifies the purposes for which personally identifiable information is to be processed; and

e. Includes BU-defined information.

6.8.b **Privacy Policies on Websites, Applications, and Digital Services - The BU shall** develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: [NIST 800 53 PM-20(1)]

a. Are written in plain language and organized in a way that is easy to understand and navigate;

b. Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and

c. Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.

6.8.c **Complaint Management** - The Bu shall Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: [NIST 800 53 PM-26]

d. Mechanisms that are easy to use and readily accessible by the public;

e. All information necessary for successfully filing complaints;

f. Tracking mechanisms to ensure all complaints received are reviewed and addressed within a BU-defined time period not to exceed CPO-defined time period;

g. Acknowledgement of receipt of complaints, concerns, or questions from individuals within BU-defined time period not to exceed CPO-defined time period; and

h. Response to complaints, concerns, or questions from individuals within BU-defined time period not to exceed CPO-defined time period.

6.9 (P) **Specific Categories of Personally Identifiable Information -** The BU shall apply specific processing conditions as required for specific categories of PII. [NIST 800 53 PT-7].

6.9.a (P) **Social Security Numbers -** When a system processes Social Security numbers, the BU shall: [NIST 800 53 PT-7(1)]

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier;

b. Not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and

c. Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

6.10 Dissemination of Privacy Program Information - The BU shall maintain a central resource webpage on the BU's principle public website that serves as a central source of information about the BU's privacy program and that: [NIST 800 53 PM-20]

a. Ensures the public has access to information about its privacy notice and is can communicate with its Privacy Officer; and

b. Ensures that BU privacy practices and reports are publicly available; and

c. Employs publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.

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 8410 SYSTEM PRIVACY

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK 8250, Media Protection

8.4 STATEWIDE POLICY FRAMEWORK 8240, Incident Response Planning

8.5 Policy (DRAFT), Document Retention

8.6 Statewide Standard 8330, System Security Audit

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

8.8 Executive Order 2008-10: Mitigating Cyber Security Threats

8.9 Arizona Revised statute; Title 12: Courts and Civil Proceedings; Article 7.1 Medical Records; Section 12-2297: Retention of records

8.10 Arizona Revised statutes; Title 41: State Government; Chapter 1: Executive Officers; Article 2.1: Arizona State Library, Archives and Public Records Established in the Office of the Secretary of State; Section 41-151.12; Records; records management; powers and duties of director; fees; records services fund

8.11 Arizona Revised statutes; Title 41: State Government; Chapter 39: Information Obtained or Disseminated by State and Local Governments; Article 1: Access to State Agency Web Site Records and Privacy: Section 41-4152.

8.12 Arizona Revised statutes; Title 41: State Government; Chapter 41: Arizona Department of Homeland Security; Article 1: General Provisions; Section 41-4172: Anti-identification procedures.

8.13 Arizona Revised statutes; Title 44: Trade and Commerce; Chapter 33: Record Discard and Disposal; Article 1: Discard and Disposal of Personal Identifying Information Records; Section 44-7601: Discarding and disposing of records containing personal identifying information; civil penalty; enforcement; definition.

8.14 General Records Retention Schedule for All Public Bodies, Information Technology (IT) Records, Schedule Number 000-12-41, Arizona State Library, Archives and Public Records, Item Numbers 10 a and b

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