STATEWIDE POLICY (8410): SYSTEM PRIVACY

DOCUMENT NUMBER:	**(P8410)**
EFFECTIVE DATE:	**DRAFT SEPTEMBER 17, 2018**
REVISION:	**2.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK 8410 SYSTEM PRIVACY.

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 information systems:

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

1.1 State Chief Information Officer (CIO) shall:

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

1.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of all (Agency) BU activities and documentation provided to ensure compliance with statewide IT 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.

5.1 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 Information Technology 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 information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

1.3 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 information systems and premises.

1.4 BU CIO shall:

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

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

1.5 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 Technology 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.

5.2 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 IT 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 information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

1.6 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.

1.7 System Users of agency information systems shall:

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

b. Adhere to PSPs regarding system privacy.

6. STATEWIDE POLICY

6.1 Authority to Collect - The BU shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or agency information system need. For additional specificity on the authority to collect, refer to Standard 8330, System Security Audit. [NIST 800 53 AP-1] [Privacy Acts] [HIPAA 164.520(a)(1)]

6.2 Purpose Specification - The BU shall describe the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. [NIST 800 53 AP-2] [HIPAA 164.520(a)(1)] [ARS 41-4152]

6.3 Access Enforcement - The BU shall ensure the agency information system enforces approved authorizations for logical access to PII in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST 800-53 AC-3]

6.4 (P) **Least Privilege** - The BU shall employ the concept of least privilege, allowing only authorized accesses to PII for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [NIST 800-53 AC-6]

6.5 **Governance and Privacy Program** - The BU shall: [NIST 800 53 AR-1]

- **a.** Appoint a Senior BU official for Privacy accountable for developing, implementing, and maintaining an organization wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and agency information systems; [HIPAA 164.530(a)(1)] [EO 2008-10]
- **b.** Monitor federal and state privacy laws for changes that affect the privacy program;
- **c.** Allocate resources to implement and operate the organization-wide privacy program;
- **d.** Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;
- **e.** Develop, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for program, agency information systems, or technologies involving PII; and
- **f.** Update privacy plan, policies, and procedures annually.

6.6 **Privacy Impact and Risk Assessment** - The BU shall: [NIST 800 53 AR-2]

- **a.** Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;
- **b.** Conduct Privacy Impact Assessments (PIAs) for agency information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any existing BU policies and procedures; and
- **c.** Ensure PIAs are conducted prior to any new collection of PII or upon significant changes in the architecture, information flow, or use of PII within existing systems.

6.7 **Privacy Requirements for Contractors and Service Providers** - The BU shall: [NIST 800 53 AR-3]

- **a.** Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and

b. Include privacy requirements in contracts and other acquisition-related documents.

6.8 Privacy Monitoring and Auditing - The BU shall monitor and audit privacy controls and internal privacy policy annually to ensure effective implementations. [NIST 800 53 AR-4]

6.9 Privacy Awareness and Training - The BU shall: [NIST 800 53 AR-5]

a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that agency employees and contractors understand privacy responsibilities and procedures;

b. Administer basic privacy training annually and targeted, role-based privacy training for agency employees and contractors having responsibility for PII or for activities that involve PII annually; and

c. Ensure that agency employees and contractors certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

6.10 Privacy Reporting - The BU shall conduct an initial evaluation, develop, disseminate, and establish and follow a schedule for regularly updating as necessary, but at least every three years, reports to the State Privacy Officer (SPO) and other appropriate oversight bodies to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. [NIST 800 53 AR-6]

6.11 Privacy-Enhanced System Design and Development - The BU shall design agency information systems to support privacy by automating privacy controls. [NIST 800 53 AR-7]

6.12 Accounting of Disclosures - The BU, consistent with state privacy acts and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 AR-8] [HIPAA 164.528(a)]

a. Keep an accurate accounting of disclosures of information 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 agency to which the disclosure was made

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.**

6.13 Data Quality - The BU shall: [NIST 800 53 DL-1]

- **a.** Confirm to the greatest extent possible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
- **b.** Collect PII directly from the individual to the greatest extent practicable;
- **c.** Check for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems annually; and
- **d.** Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

6.14 Data Integrity - The BU shall: [NIST 800 53 DI-2]

- **a.** Document processes to ensure the integrity of PII through existing security controls.

6.15 Minimization of Personally Identifiable Information - The BU shall: [NIST 800 53 DM-1]

- **a.** Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
- **b.** Limit the collections and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and
- **c.** Conduct an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least every three years and update as necessary to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

6.16 Data Retention and Disposal - The BU shall: [NIST 800 53 DM-2]

- **a.** Retain each collection of PII for BU-defined time period to fulfill the purposes identified in the notice or as required by law, refer to Policy DRAFT, Document Retention;
- **b.** Dispose of, destroy, erases, and/or anonymize the PII, regardless of the method of storage, in accordance with an Arizona State Library-approved record retention schedules and in a manner that prevents loss, theft, misuse, or unauthorized access; and [ARS 44-7601] [ARS 41-151.12]
- **c.** Use techniques, documented in the Policy 8250, Media Protection, to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

6.17 Consent - For collection, use, and disclosures of PII not already authorized by law the BU shall: [NIST 800 53 IP-1]

- **a.** 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)]
- **b.** Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
- **c.** Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII;
- **d.** Ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

6.18 Individual Access - The BU, consistent with the laws and regulations, and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 IP-2] HIPAA 164.524(a)]

- **a.** Provide individuals the ability to have access to their PII maintained in its system(s) of records;
- **b.** 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)]
- **c.** Adhere to requirements and policies and guidance for the proper processing of PII requests.

6.19 Redress - For collection, use, and disclosures of PII not already authorized by law the BU shall: [NIST 800 53 IP-3] [HIPAA 164.526(a)-(f)]

- **a.** Provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and
- **b.** Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals.

6.20 Complaint Management - For collection, use, and disclosures of PII not already authorized by law the BU shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about the (Agency) BU privacy practices. [NIST 800 53 IP-4] [HIPAA 164.530(d)]

6.21 Inventory of PII - The BU Privacy Officer shall: [NIST 800 53 SE-1]

a. Establish, maintain, and update at least every three years an inventory that contains a listing of all programs and BU information systems identified as collecting, using, maintaining, or sharing PII; and

b. Provide each update of the PII use to the BU CIO or BU ISO at least every three years to support the establishment of information security requirements for all new or modified BU information systems containing PII.

6.22 Privacy Incident Response - The BU shall: [NIST 800 53 SE-2]

a. Develop and implement a Privacy Incident Response Plan consistent with requirements in STATEWIDE POLICY FRAMEWORK 8240 Incident Response Planning; and

b. Provide an organized and effective response to privacy incidents in accordance with the BU Privacy Incident Response Plan.

6.23 Privacy Notice - The following guidance is offered for the development of a Privacy Notice: [NIST 800 53 TR-1] [HIPAA 164.520(c)] [ARS 41-4152]

a. Provides effective notice to the public and to individuals regarding:

b. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;

c. Authority for collection PII;

d. The choices, if any, individuals may have regarding how the (Agency) BU uses PII and the consequences of exercising or not exercising those choices;

e. The ability to access and have PII amended or corrected if necessary;

f. Describes the following:

1. How the PII the BU collects and the purpose(s) for which it collects that information;

2. How the BU uses PII internally;

3. Whether the BU shares PII with external entities, the categories of those entities, and the purposes for such sharing;

4. Whether individuals have the ability to consent to specific uses of sharing of PII and how to exercise any such consent;

5. How individuals may obtain access to PII; and

6. How the PII will be protected.

g. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change; and

h. Provides notice in clear and conspicuous language when individuals are first asked to provide PII to the BU.

6.24 Dissemination of Privacy Program Information - The BU shall: [NIST 800 53 TR-3]

a. Ensure the public has access to information about its privacy notice and is able to communicate with its Privacy Officer; and

b. Ensure that its privacy notice are publicly available through BU websites or publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy notice.

6.25 Internal Use - The BU shall use PII internally only as authorized by law or for the authorized purpose(s) described in privacy notice. [NIST 800 53 UL-1]

6.26 Information Sharing with Third Parties - The BU shall: [NIST 800 53 UL-2] [HIPAA 164.508(a)]

a. Share PII externally, only as authorized by law or for the authorized purposes identified and described in privacy notice or in a manner compatible with those purposes;

b. Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, Service Level Agreements, Business Associate Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used and offers the same level of protection as documented in this policy; [HIPAA 164.514(e)(4)]

c. Monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use of sharing of PII; and

d. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new privacy notice is required.

7. DEFINITIONS AND ABBREVIATIONS

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

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 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

8.8 Executive Order 2008-10: Mitigating Cyber Security Threats

8.9 Arizona Revised Statue; Title 12: Courts and Civil Proceedings; Article 7.1 Medical Records; Section 12-2297: Retention of records

8.10 Arizona Revised Statues; 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 Statues; 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 Statues; 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 Statues; 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 Arizona State CIO
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed Arizona State CIO
9/17/2018	Updated for PCI-DSS 3.2.1	2.0	Morgan Reed, State of Arizona CIO and Deputy Director