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**
1/16/2024	**Annual Updates**	**4.0**	Ryan Murray (Jan 16, 2024 17:09 MST)

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

P8410_System_Privacy (2)

Final Audit Report 2024-01-17

Created:	2024-01-16
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGGHAIj0Nzv834eVCeV7nZxFZoNeO7JnI

"P8410_System_Privacy (2)" History

Document created by Ed Yeargain (eyeargain@azdohs.gov)
2024-01-16 - 11:34:05 PM GMT

Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature
2024-01-16 - 11:35:09 PM GMT

Document e-signed by Ryan Murray (rmurray@azdohs.gov)
Signature Date: 2024-01-17 - 0:09:25 AM GMT - Time Source: server

Agreement completed.
2024-01-17 - 0:09:25 AM GMT