ARIZONA STATEWIDE INFORMATION SECURITY	STATEWIDE POLICY	State of Arizona

STATEWIDE POLICY 8270: PERSONNEL SECURITY PROTECTIONS

DOCUMENT NUMBER:	P8270
EFFECTIVE DATE:	JULY 1, 2015
REVISION:	DRAFT

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-3504 and§ 41-3507.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit to protect state information systems and assets containing sensitive data through personnel security controls.

3. SCOPE

3.1 Application to Budget Units - This policy shall apply to all budget units (BUs) as defined in A.R.S. § 41-3501(1).

3.2 Application to Systems - This policy shall apply to all state information systems:

- **a. (P)** Policy statements preceded by "(P)" are required for state information systems categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for state information systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for state information systems with protected healthcare information.
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for state 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 subject matter experts shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of all state BU activities and documentation provided to ensure compliance with statewide IT 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 State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Budget Unit (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 state information systems and assets.

5.4 BU Chief Information Officer (CIO) shall:

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

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

5.5 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 IT 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 state information systems and assets through personnel security controls.

5.6 Supervisors of state employees and contractors shall:

a. Ensure users are appropriately trained and educated on Personnel Security Policies; and

b. Monitor employee activities to ensure compliance.

5.7 Users of state information systems shall:

a. Familiarize themselves with this and related PSPs; and

b. Adhere to PSPs regarding the protection of state information 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 state information systems. Examples of sensitive positions include: [NIST 800-53 PS-02] [IRS Pub 1075]

1. Firewall administrator

2. Members of the incident response team

3. Those with vulnerability scanning duties

6.2 Position Definition - The BU shall define information security responsibilities for all personnel. [HIPAA(a)(3)(ii)(A), (a)(3)(ii)(B) - Addressable] [PCI 12.4]. Specifically, the following information security responsibilities:

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

b. Individual or team responsible for monitoring and analyzing security alerts and information, and distributing to appropriate employees and contractors; [PCI 12.5.2]

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

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

e. Individual or team responsible for monitoring and controlling all access to data. [PCI 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-03] [IRS Pub 1075] [PCI 12.7]

6.4 Personnel Separation - Upon separation of individual employment, the BU shall: [NIST 800-53 PS-04] [HIPAA(a)(3)(ii)(C)]

a. Terminate state information system access within 24 hours;

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

c. Retrieve all security-related state information system-related property;

d. Retain access to state information system accounts formerly controlled by terminated individual; and

e. Allow the terminated individual access to authorized services such as benefits, reimbursement, and retirement information, according to BU policies or State policies.

6.5 Personnel Transfer - The BU shall: [NIST 800-53 PS-05] [IRS Pub 1075]

a. Review logical and physical access authorization to state information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates returning old and reissuing new keys, identification cards, and building passes;

b. Close previous information system accounts and establish new accounts;

c. Change state information system access authorizations;

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

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

6.6 Access Agreements - The BU shall ensure that individuals requiring access to state information systems acknowledge and accept appropriate access agreement prior to being granted access and reviews/updates the access agreements annually. [NIST 800-53 PS-06] [IRS Pub 1075] [PCI 12.3].

6.7 Third-Party Personnel Security - The BU shall: [NIST 800-53 PS-07] [IRS Pub 1075] [HIPAA 164.314(a)(1)]

a. Establish personnel security requirements including security roles and responsibilities for third-party providers;

b. Documents personnel security requirements; and

c. Monitor provider compliance.

6.8 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.

6.9 Personnel Sanctions - The BU shall employ a formal sanctions process for personnel failing to comply with established state information security and privacy PSPs and document the sanctions applied. [NIST 800-53 PS-08] [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 website.

8. REFERENCES

8.1 Statewide Policy Exception Procedure

8.2 Executive Order 1403

8.3 A.R.S. 41-710

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

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) v2.0, PCI Security Standards Council, October 2010.

8.7 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
5/1/14	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director