ARIZONA STATEWIDE INFORMATION SECURITY	STATEWIDE STANDARD	State of Arizona

STANDARD 8220: SYSTEM SECURITY MAINTENANCE POLICY

DOCUMENT NUMBER:	S8220
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.)§ 18-104 and § 18-105.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

3.1 **Application to Budget Units (BUs)** - This standard shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 **Application to Systems** - This standard shall apply to all state information systems. Standard statements preceded by "(P)" are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

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.

4.2 (Agency) BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology 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 information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Statewide Information Technology 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 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 System Security Maintenance Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 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 Technology PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the System Security Maintenance Policy for the BU state information systems; and

c. Ensure all personnel understand their responsibilities with respect to secure system management and maintenance.

6. STATEWIDE POLICY

6.1 Baseline Configuration - The BU shall develop, document, and maintain a current baseline configuration of each state information system. The baseline configuration shall

6.1.1 Development of Configuration Baselines - BUs may develop their own configuration baselines or utilize authoritative sources such as the United States Government Configuration Baseline (USGCB). The USGCB is a set of configuration baselines for widely used Information Technology (IT). BUs are ultimately responsible for ensuring that the USGCB (or other authoritative source) settings for IT deployed in their agency are properly tested and implemented. Customization of these baselines is expected to support BU functional requirements and their unique operating environment.

6.1.2 Documentation of Baseline - BUs shall document the configuration baselines for their IT. When referring to USGCB (or other authoritative sources) configuration settings as the documentation for deployed systems, the USGCB version and all exceptions must be noted.

6.1.3 Use of Configuration Scanners - BUs are encouraged to utilize automated means of confirming configuration settings for deployed IT. The NIST Security Content

Automation Protocol (SCAP) validation program ensures configuration scanning tools meet the SCAP protocol. BUs are encourage to use SCAP-validated tools.

6.2 **(P) Baseline Configuration for High Risk Areas** - The BU issues laptops with sanitized hard drives, hard disk encryption, and two-factor authentication, to individuals traveling to locations the BU deems to be of significant risk.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 NIST 800-70 Rev. 2, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers, February 2011.

8.2 ARS 44-7041

8.3 Arizona State Library Retention Schedules

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

8.6 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
01/01/2014	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director