

ARIZONA DEPARTMENT OF ADMINISTRATION	<h1>STATEWIDE POLICY</h1>	 State of Arizona
---	-------------------------------	---

STATEWIDE POLICY (8220): SYSTEM SECURITY MAINTENANCE

DOCUMENT NUMBER:	(P8220)
EFFECTIVE DATE:	OCTOBER 11, 2016
REVISION:	1.0

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration, 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 8220 SYSTEM SECURITY MAINTENANCE.

2. PURPOSE

The purpose of this policy is to establish the baseline controls for management and maintenance of agency information 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 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 subject matter experts 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

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 Agency 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 agency 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 Agency 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 Agency Information Technology PSPs;
- b. Ensure the development and implementation of an adequate controls enforcing the System Security Maintenance Policy for the BU agency information 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 information systems that will:

- a. Address the roles, responsibilities, and configuration management processes and procedures;

- b. Establish a process for identifying configuration items throughout the software development lifecycle and for managing the configuration of the configuration items;
- c. Define the configuration items for the agency information system and place the configuration items under configuration management; and
- d. 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 information system. [NIST 800 53 CM-2]

6.1.2.1 (P) **Baseline Configuration Reviews and Updates** - The BU shall review and update the baseline configurations for information 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 (1)] [Internal Revenue Service (IRS) Pub 1075]

6.1.2.2 (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](http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf) Item 8.

6.1.2.3 (P) **Baseline Configuration for High Risk Areas** - The BU shall establish separate baseline configurations for identified high risk areas. [NIST 800-53 CM-2 (7)] [IRS Pub 1075]

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

- a. Determine the types of changes to the agency information system that are configuration-controlled;
- b. Review proposed configuration-controlled changes to the agency information system and approves or disapproves such changes with explicit consideration for security impact analysis;
- c. Document configuration change decisions associated with the agency information system;
- d. Implement approved configuration-controlled changes to the information system;

- e. Retain activities associated with configuration-controlled changes to the agency information 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](http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf) Item 8; and
- f. 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 information systems.

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

- 6.1.4.1 (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-4 (3)] [IRS Pub 1075]

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 information systems. The BU shall permit only qualified and authorized individuals to access agency information 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 information technology products employed within the agency information 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 information 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 Information System Component Inventory - The BU shall develop and document an inventory of agency information system components (including authorized wireless access points and business justification for those access points)

that accurately reflects the current agency information system, is consistent with the defined boundaries of the agency information 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. [NIST 800 53 CM-8] [PCI DSS 2.4 , 11.1.1]

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

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

6.1.7.3 **(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 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 Information System Maintenance - In addition to the change management requirements of Section 6.1, the following requirements apply to the maintenance of agency information systems:

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

- a. Schedule, perform, document, and review records of maintenance and repairs on agency information system components in accordance with manufacturer or vendor specifications and BU requirements;

- b. Approve and monitor all maintenance activities whether performed onsite or remotely and whether the equipment is serviced onsite or removed to another location;
- c. Explicitly approve the removal of the agency information system or system components from the BU facilities for offsite maintenance or repair;
- d. 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
- e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. These checks are documented in BU maintenance records.

6.2.2 (P) Maintenance Tools - The BU shall approve, control, and monitor agency information system maintenance tools. [NIST 800 53 MA-3] [IRS Pub 1075]

6.2.2.1 **(P) Tool Inspection** - Maintenance tools, and/or diagnostic and test programs carried into a BU facility by maintenance personnel shall be inspected for improper or unauthorized modifications including malicious code prior to the media being used in the agency information system. [NIST 800 53 MA-3(1)(2)] [IRS Pub 1075]

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 information 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](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.

6.2.3.1 **(P) Remote Maintenance Policies and Procedures** - The BU shall document in the security plan for the agency information system the policies and procedures for the installation and use of remote

maintenance and diagnostics are documented connections. (See Information Security Program Policy P8120) [NIST 800 53 MA-4(2)] [IRS Pub 1075]

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 information 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.

6.3 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 information 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 the state of the information system components with regard to flaw remediation. [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. Employ centrally managed malicious code protection mechanisms at agency information 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(2)] [PCI DSS 5.1, 5.1.1]
 - i. 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]

- b. 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(1)]
- c. Address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of the agency information system; and
- d. Configure malicious code protection mechanisms to:
 - i. Perform periodic scan of the agency information 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]
 - ii. Block and quarantine malicious code and/or send an alert to a system administrator in response to malicious code detection; and
 - iii. Generate audit logs. [PCI DSS 5.2]
 - iv. 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 Information 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 information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections;
- b. Identify unauthorized use of the agency information system through BU-defined intrusion-monitoring tools;
- c. Deploy monitoring devices strategically within the agency information system, including at the perimeter and critical points inside the environment to collect essential security-relevant data and to track specific types of transactions of interest to the BU; [PCI DSS 11.4]
- d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. Heighten the level of monitoring activity within the intrusion monitoring systems whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the agency based on Confidential information;
- f. Receive alerts from malicious code protection mechanisms;
- g. Receive alerts from intrusion detection or prevention systems;

- h. Receive alerts from boundary protection mechanisms such as firewalls, gateways, and routers; and
- i. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations.

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 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 Traffic - The BU shall 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 implement the information monitoring system to alert system administrators when the following indications 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 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 system files, configuration files, or content files. [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 information systems will perform integrity checks at least weekly and at start up, the identification of a new threat to which agency information 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) **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 information 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 SI-8(1)] [IRS Pub 1075]

6.3.8 (P) Information Input Validation - The BU shall ensure agency information systems check the validity of information 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 information 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 Output Handling and Retention - The BU shall handle and retain information within the agency information 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]

6.4 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 website.

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** NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.
- 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, 2010.
- 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