ARIZONA STATEWIDE INFORMATION SECURITY	STATEWIDE POLICY	State of Arizona

STATEWIDE POLICY (8330): SYSTEM SECURITY AUDIT

DOCUMENT NUMBER:	**(P8330)**
EFFECTIVE DATE:	**OCTOBER 11, 2016**
REVISION:	**1.0**

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 8330 SYSTEM SECURITY AUDIT.

2. PURPOSE

The purpose of this policy is to protect agency information systems and data by ensuring the Budget Unit (BU) and agency information systems have the appropriate controls and configurations to support audit log generation, protection, and review.

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 - 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 - Prior to selecting and procuring information technology products and services, BU SMEs shall consider and 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 Audit 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 Audit Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 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 Security Audit Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the generation, protection and review of audit logs.

5.6 Supervisors of agency employees and contractors shall:

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

b. Monitor employee activities to ensure compliance.

5.7 System Users of agency information systems shall:

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

b. Adhere to PSPs regarding the generation, protection and review of audit logs.

6. POLICY

6.1 **Audit Events** -The BU shall: [NIST 800-53 AU-2]

a. Determine that the agency information system is capable of auditing the events listed in the Statewide System Security Audit Standard S8330.

b. Coordinate the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Ensure the events listed in the Statewide System Security Audit Standard S8330 are logged within the agency information system.

6.1.1 **(P) Audit Reviews and Updates** - The BU shall review and update the selected audited events annually, or as required. [NIST 800-53 AU-2(3)] [IRS Pub 1075]

6.2 **Content of Audit Records** - The BU shall ensure the agency information system generates audit records containing information that establishes: [NIST 800-53 AU-3]

a. What type of event occurred; [PCI DSS 10.3.2] [IRS Pub 1075]

b. When the event occurred; [PCI DSS 10.3.3] [IRS Pub 1075]

c. Where the event occurred; [PCI DSS 10.3.5] [IRS Pub 1075]

d. The source of the event (i.e., name of the affected data, system component, or resource); [PCI DSS 103.6] [IRS Pub 1075]

e. The outcome of the event; and [PCI DSS 10.3.4]

f. The identity of any individuals or subjects associated with the event. [PCI DSS 10.3.1] [IRS Pub 1075]

6.2.1 (P) Additional Audit Information - The BU shall ensure the state information system generates audit records containing BU-defined additional information. [NIST 800-53 AU-3(1)] [IRS Pub 1075]

6.3 **Audit Storage Capacity** - The BU shall allocate audit record storage capacity in accordance with BU-defined audit record storage requirements. [NIST 800-53 AU-4]

6.4 **Response to Audit Processing Failures** - The BU shall ensure the agency information system alerts BU-defined personnel or roles in the event of an audit processing failure; and shuts down the agency information system, overwrites the oldest audit records, or stops generating audit records. [NIST 800-53 AU-5]

6.5 **Audit Review, Analysis, and Reporting** - The BU shall review and analyze agency information system audit records periodically for indications of inappropriate or unusual activity; and reports findings to BU-defined personnel or roles. Agency information systems with cardholder data (CHD) shall perform this review daily. [NIST 800-53 AU-6] [HIPAA 164.308 (a)(1)(ii)(D)] [HIPAA 164.312 (b)] [PCI DSS 10.6]

6.5.1 (P) **Process Integration** - The BU shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. [NIST 800-53 AU-6(1)] [IRS Pub 1075]

6.5.2 (P) **Correlate Audit Repositories** - The BU shall analyze and correlate audit records across different repositories to gain BU-wide situational awareness. [NIST 800-53 AU-6(3)] [IRS Pub 1075]

6.6 Audit Reduction and Report Generation - The BU shall ensure the agency information system provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter original audit records. [NIST 800-53 AU-7]

6.6.1 (P) **Automatic Processing** - The BU shall ensure the agency information system provides the capability to process audit records for events of interest based on the following audit fields within audit records: [NIST 800-53 AU-7(1)] [IRS Pub 1075]

- **a.** Individual identities
- **b.** Event types
- **c.** Event locations
- **d.** Event times and time frames
- **e.** Event dates
- **f.** System resources involved, IP addresses involved
- **g.** Information object accessed

6.7 Time Stamps - The BU shall ensure the agency information system uses internal system clocks to generate time stamps for audit records; and generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and provides a granularity of time to a BU-defined unit of time. [NIST 800-53 AU-8]

6.7.1 (P) **Synchronization with Authoritative Time Source** - The BU shall ensure the agency information system synchronizes internal agency information system clocks a BU-defined frequency with a BU-defined time source when the time difference is greater than a BU-defined time period. [NIST 800-53 AU-8(1)] [IRS Pub 1075] [PCI DSS 10.4.1, 10.4.3]

6.7.2 (P) **Protection of Time Data** - The BU shall ensure the agency information system protects time-synchronization settings by restricting access to such settings to authorized personnel and logging, monitoring, and reviewing changes. [PCI DSS 10.4.2]

6.8 Protection of Audit Information - The BU shall ensure the agency information system protects audit information and audit tools from unauthorized access, modification, and deletion. [NIST 800-53 AU-9] [PCI DSS 10.5] [IRS Pub 1075]

6.8.1 (P) **Access by Subset of Privileged Users** -The BU shall authorize access and modification to management of audit functionality to only a BU-defined subset of privileged users. [NIST 800-53 AU-9(4)] [IRS Pub 1075] [PCI DSS 10.5.1, 10.5.2]

6.8.2 (P) **Audit Trail Backup** - The BU shall promptly back up audit trail files to a centralized log server or media that is difficult to alter. [PCI DSS 10.5.3]

6.8.3 (P) **Audit Backup on Separate Physical Systems** - The BU shall ensure the agency information system backs up audit records onto a physically different system or system components than the system or component being audited. [PCI DSS 10.5.4]

6.8.4 (P) **File Integrity Monitoring of Audit Logs** - The BU shall ensure the agency information system uses file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts. [PCI DSS 10.5.5]

6.9 **Audit Record Retention** - The BU shall retain audit records for a BU-defined time period with a BU-defined time period available for immediate analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. For agency information systems with cardholder data these defined times are at least one year with a minimum of three months immediately available for analysis. [NIST 800-53 AU-11] [PCI DSS 10.7] 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 16.b.

6.10 **Audit Generation** - The BU shall ensure the agency information system: [NIST 800-53 AU-12]

a. Provides audit record generation capability for the auditable events, defined in Section 6.1 (Audit Records), at servers, firewalls, workstations, and other BU-defined system components;

b. (P) Anti-virus programs are generating audit logs; [PCI DSS 5.2]

c. Allows BU-defined personnel or roles to select which auditable events are to be audited by specific components of the agency information system; and

d. Generates audit records for the events, defined in Section 6.1 (Audit Events), with the content defined in Section 6.2 (Content of Audit Records).

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 8330 SYSTEM SECURITY AUDIT

8.2 Statewide Policy Exception Procedure

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

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.

8.7 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 Number 16b

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change
9/01/2014	Initial Release
10/11/2016	Updated all the Security Statut