STATEWIDE

POLICY

State of Arizona

STATEWIDE POLICY (8330): SYSTEM SECURITY AUDIT

DOCUMENT NUMBER:	**P8330**
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 policy is to protect agency systems and data by ensuring the Budget Unit (BU) and agency systems have the appropriate controls and configurations to support audit log generation, protection, and review.

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.

4.1.1 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 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 the BU activities and documentation provided to ensure compliance with statewide information security 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 Director the risk to state systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of Agency Information Security 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 systems and assets.

5.5 BU Chief Information Officer (CIO) shall:

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

b. Ensure System Security Audit Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 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 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.

5.7 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.

5.8 System Users of agency 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. STATEWIDE POLICY

6.1 Event Logging -The BU shall: [NIST 800-53 AU-2]

a. Identify the types of events the agency system is capable of logging in support of the audit function. .

b. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection of criteria for events to be logged;

c. Specify the event types for logging within the system as defined in the Statewide System Security Audit Standard S8330 along with the frequency of logging for each identified event type;

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents;

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

f. Review and update the event types selected for logging annually; and [IRS Pub 1075]

g. (P) For agencies that provide a shared hosting service to other agencies, ensure that logging and audit trails are unique to each agencies environment. [PCI DSS A.1.3]

6.1.1 Content of Audit Records - The BU shall ensure the agency systeminformation system generates audit records containing information that establishes: [NIST 800-53 AU-3] [PCI DSS 10.3]

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 10.3.6] [IRS Pub 1075]

e. The outcome of the event; and [PCI DSS 10.3.5]

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

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

6.1.3 **Limit Personally Identifiable Information Elements** - The BU shall limit personally identifiable information contained in audit records to the BU-defined elements identified in the privacy risk assessment. [NIST 800-53 AU-3(3)

6.2 **Audit Storage Capacity** - The BU shall allocate audit log storage capacity to accomodate BU-defined audit log storage requirements. [NIST 800-53 AU-4]

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

6.3.1 (P) **Storage Capacity Warning** - The BU shall ensure the agency system provides a warning to BUI-defined personnel when allocated audit log storage volume reaches a maximum capacity. [NIST 800-53 AU-5(1)] [IRS Pub 1075]

6.4 **Audit Review, Analysis, and Reporting** - The BU shall: [NIST 800-53 AU-6] [HIPAA 164.308 (a)(1)(ii)(D)] [HIPAA 164.312 (b)]

a. eview and analyze agency system audit records periodically for indications of inappropriate or unusual activity and the potential impact;

b. Report findings to BU-defined personnel or roles; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

d. (P-PCI) Agency systems with cardholder data (CHD) shall perform this review daily. [PCI DSS 10.6, 10.6.1, 10.6.2, 10.6.3]

6.4.1 (P) **Process Integration** - The BU shall integrate audit record review, analysis, and reporting processes using automated mechanisms. [NIST 800-53 AU-6(1)] [IRS Pub 1075]

6.4.2 (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]

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

6.5.1 (P) **Automatic Processing** - The BU shall ensure the agency system provides and implements the capability to process, sort, and search 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

6.6 **Time Stamps** - The BU shall ensure the agency system uses internal system clocks to generate timestamps for audit records; and records time stamps for audit records that meet the BU-defined granularity of time measurement and that can use Coordinated Universal Time (UTC), Greenwich Mean Time (GMT), or have a fixed local time offset from UTC or GMT, or that include the local time offset as part of the time stamp. [NIST 800-53 AU-8]

6.6.1 (P) **Synchronization with Authoritative Time Source** - The BU shall ensure the agency system compares the internal agency system clocks a BU-defined frequency with a BU-defined time source and synchronizes the internal agency system clocks to the authoritative time source when the time difference is greater than a BU-defined time period. [NIST 800-53 SC-45(1)] [PCI DSS 10.4, 10.4.1, 10.4.3]

6.6.2 (P) **Protection of Time Data** - The BU shall ensure the agency 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]

6.7 **Protection of Audit Information** - The BU shall ensure the agency system protects audit information and audit logging tools from unauthorized access, modification, and deletion; and alerts BU-defined personnel upon detection of unauthorized access, modification, or deletion of audit information. [NIST 800-53 AU-9] [PCI DSS 10.5] [IRS Pub 1075]

6.7.1 (P) **Access by Subset of Privileged Users** -The BU shall authorize access and modification to management of audit logging 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]

6.7.2 (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]

6.7.3 (P) **Audit Backup on Separate Physical Systems** - The BU shall ensure the agency 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]

6.7.4 (P) **File Integrity Monitoring of Audit Logs** - The BU shall ensure the agency 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]

6.8 **Audit Record Retention** - The BU shall retain audit records for a BU-defined time period consistent with the records retention policy with a BU-defined time period available for immediate analysis to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. For agency 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.

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

a. Provides audit record generation capability for the event types, defined in Section 6.1.a (Event Loggins), at servers, firewalls, workstations, mobile devices, and other BU-defined system components and services;

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

c. Allows BU-defined personnel or roles to select the event types that are to be logged by specific components of the agency system; and

d. Generates audit records for the event types, defined in Section 6.1.c (Event Loggings), with the content defined in Section 6.2 (Content of Audit Records).

6.10 (P) **Cross Agency Auditing** - The BU shall employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across BU boundaries. Note: This requirement applies to outsourced data centers and cloud service providers. The provider must be held accountable to protect and share audit information with the BU through the contract. [NIST 800 53 AU-16]

6.11 (P) **Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for monitoring all access to network resources and Confidential data are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 10.9]

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 8330 SYSTEM SECURITY AUDIT

8.2 Statewide Policy Exception Procedure

8.3 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

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) v3.2.1, PCI Security Standards Council, May 2018.

8.6 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

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	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

P8330_System_Security_Audit (1)

Final Audit Report 2024-01-17

Created:	2024-01-16
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAICFa9m47xNrvKTbccQWyAp9swfWnQLC2

"P8330_System_Security_Audit (1)" History

Document created by Ed Yeargain (eyeargain@azdohs.gov)

2024-01-16 - 11:35:50 PM GMT

Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature

2024-01-16 - 11:36:47 PM GMT

Document e-signed by Ryan Murray (rmurray@azdohs.gov)

Signature Date: 2024-01-17 - 0:09:12 AM GMT - Time Source: server

Agreement completed.

2024-01-17 - 0:09:12 AM GMT