STATEWIDE

STANDARD

State of Arizona

STATEWIDE STANDARD (8330): SYSTEM SECURITY AUDIT

DOCUMENT NUMBER:	**S8330**
EFFECTIVE DATE:	**April 5, 2024**
REV:	**1.1**

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 standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

3.1 **Application to Budget Units** - This standard applies to all Budget Units (BUs). A BU is defined as a department, commission, board, institution or other agency of the state receiving, expending or disbursing state funds or incurring obligations of the state including the Arizona Board of Regents but excluding the universities under the jurisdiction of the Arizona Board of Regents, the community college districts and the legislative or judicial branches. A.R.S. § 41-3501(2).

3.2 **Application to Systems** - This standard shall apply to all state information 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 **Federal Government Information** - 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 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	Rationale

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of statewide 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) shall:

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 **Audit Events** – The BU shall ensure state information systems are capable of auditing the minimum set of events that may be required to support the BU's auditing policy and those events listed under the "System Audit Capabilities" column in the table below. In addition, the BU shall also ensure that the state information system is configured to audit the minimum set of events listed under the "System Audited Events" column in the table below. [NIST 800-53 AU-2]

System Audit Capabilities	System Audited Events
● Password changes;	● Password changes;
● Successful and failed logons; [PCI DSS 10.2.5]	● Successful and failed logons; [PCI DSS 10.2.5] [IRS Pub 1075]
● **(P)** Successful system component access; [PCI DSS 10.1] ● Failed system component access;	● **(P-PCI)** Successful system component access; [PCI DSS 10.1] ● Failed system component accesses;
● Administrative privilege usage; ● All actions taken by individuals with root or administrative privilege; [PCI DSS 10.2.2]	● Administrative privilege usage including changes to administrative account, administrative group account, escalation of user account to administrator account, and adding or deleting users from the administrator group accounts; [IRS Pub 1075] ● **(P)** All actions taken by individuals with root or administrative privilege; [PCI DSS 10.2.2] [IRS Pub 1075]
● Third-party credential usage;	● Third-party credential usage;
● Successful and failed access to system objects (e.g., files);	● **(P-PCI)** Failed or successful access to system objects with Confidential data; [PCI DSS 10.2.1, 10.2.4]
● Initialization or disabling of audit logs; [PCI DSS 10.2.6] [IRS Pub 1075]	● Initialization or disabling of audit logs; [PCI DSS10.2.6] [IRS Pub 1075]
● Access to audit trails; [PCI DSS 10.2.3]	● Access to audit trails; [PCI DSS 10.2.3] [IRS Pub 1075]
● Creation or deletion of system-level objects; [PCI DSS 10.2.7]	● **(P-PCI)** Creation or deletion of system-level objects; [PCI

	DSS 10.2.7]
	● **(P-FTI)** All changes to access control (e.g., rights, permissions); [IRS Pub 1075] ● (P-FTI) Creation, modification, and deletion of objects including files, directories, user accounts, group accounts, and account privileges; [IRS Pub 1075] ● (P-FTI) Start up and shutdown functions; and [IRS Pub 1075] ● (P-FTI) Command line changes, batch file changes and system queries. [IRS Pub 1075]

6.2 **Unsuccessful Login Attempts** – The state information system enforces the following parameters for unsuccessful login attempts:

Parameter	Value
Limit of consecutive invalid login attempts	6
Response to over limit invalid attempts	Automatically lock account/node
Lock-out period	30 minutes or release by administrator

6.3 **(P) Session Lock** – The state information system prevents further access to the system by enforcing the following parameters for session locks:

Parameter	Value
Initiate lock session after defined duration of inactivity or on user request	15 minutes
Retain session lock for defined duration or until user reestablishes access	30 minutes
Result of user not reestablishing session	Session dropped

7. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

None.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	**Initial Release**	**1.0**	**Aaron Sandeen, State CIO and Deputy Director**
04/05/2024	**Review**	**1.1**	Ryan Murray (Apr 5, 2024 09:32 PDT) **Ryan Murray, Deputy Director of Arizona Department of Homeland Security & Interim State Chief Information Security Officer**