ARIZONA STATEWIDE SECURITY STANDARD	STATEWIDE STANDARD	State of Arizona

Standard: System Security Audit

DOCUMENT NUMBER:	S8330
EFFECTIVE DATE:	JULY 1, 2015
REV:	DRAFT

1. AUTHORITY

The authority for this standard is based on Arizona Revised Statutes (A.R.S.) 41-3504: Powers and duties of the department. The Arizona Department of Administration (ADOA) develops, implements, and maintains a coordinated statewide plan for information technology. This includes adopting statewide technical, coordination and security standards for information technology. A.R.S. § 41-3504, A.R.S. § 41-3507.

2. PURPOSE

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

3. SCOPE

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).

3.1.1 **Application to Systems** – The standard applies to all state information systems. Categorization of systems is defined within the Information Security Program Policy.

a. **(P)** Policy statements preceded by "(P)" are required for state information systems categorized as Protected.
b. **(P-PCI)** Policy statements preceded by "(P-PCI)" are required for state information systems with payment card industry data (e.g., cardholder data).
c. **(P-PHI)** Policy statements preceded by "(P-PHI)" are required for state information systems with protected healthcare information.

d. **(P-FTI)** Policy statements preceded by "(P-FTI)" are required for state information systems with federal taxpayer information.

4. EXCEPTIONS

None.

5. ROLES AND RESPONSIBILITIES

Refer to associated Policy (P8330 – System Security Audit Policy).

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 administrative 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	• Initialization or disabling of audit logs; [PCI DSS

logs; [PCI DSS 10.2.6] [IRS Pub 1075]	10.2.6] [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 Logon Attempts – The state information system enforces the following parameters for unsuccessful logon attempts:

Parameter	Value
Limit of consecutive invalid logon 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 website.

8. REFERENCES

NONE

9. ATTACHMENTS

NONE