ARIZONA **S**TATEWIDE **S**ECURITY **P**olicies	**STATEWIDE** **POLICY**	**State of Arizona**

Policy XXXX: User Owned Devices

DOCUMENT NUMBER:	**PXXX**
EFFECTIVE DATE:	**DRAFT**
REVISION:	**DRAFT**

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.

2. PURPOSE

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

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 state information systems. Policy statements preceded by "(P)" are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

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 ADOA Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. ADOA 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 ADOA Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, ADOA BU SMEs shall consider ADOA and Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

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 all state BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs;

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; and

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Statewide Information Technology PSPs within the BU;

b. Ensure BU compliance with Information Security Program Policy; and

c. Promote efforts within the BU to establish and maintain effective use of

state 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 Statewide Information Technology PSPs within the BU;
- **b.** Ensure information security risks to Protected state information systems, are adequately addressed according to the Protected state information system risk assessment documentation; and
- **c.** Be system owner for all state information systems or delegate a system owner for BU state information system.

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 BU Information Technology PSPs;
- **b.** Ensure the development and implementation of adequate controls enforcing the BU PSPs; and
- **c.** Request changes and/or exceptions to existing Statewide PSPs from the State CISO.

5.6 System Users of agency information systems shall:

- **a.** Become familiar with this and related PSPs; and
- **b.** Adhere to PSPs regarding classification of data and handling within agency information systems.

6. STATEWIDE POLICY

6.1 Use of user owned devices to access State data and systems shall comply with agency and Statewide IT Security policies and standards.

6.2 (P) Use of user owned devices to access State data classified as confidential shall comply with agency and Statewide IT Security policies and standards marked as (P) and required for BU information systems categorized as Protected.

6.3 Employees must acknowledge a user owned device use agreement.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA website.

8. REFERENCES

8.1 Statewide Policy Exception Procedure

8.2 Statewide IT Security policies and standards
(https://aset.az.gov/resources/policies-standards-and-procedures)

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
11/26/18	Initial Release	DRAFT	