



STATEWIDE POLICY 8250: MEDIA PROTECTION

DOCUMENT NUMBER:	P8250
EFFECTIVE DATE:	JULY 1, 2015
REVISION:	DRAFT

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the BU 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.) § 41-3504 and A.R.S. § 41-3507.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit (BU) to ensure the secure storage, transport, and destruction of sensitive information.

3. SCOPE

3.1 Application to Budget Units (BUs) - This policy shall apply to all BUs as defined in A.R.S. § 41-3501(1).

3.2 Application to Systems - This policy shall apply to all state information systems:

- 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.

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

- a. BU subject matter experts (SMEs) should inquire with the vendor and the state or BU 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 subject matter experts shall consider 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 Statewide Information Technology (IT) PSPs throughout all state budget units (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 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; 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 Statewide Information Technology PSPs within the BU;
- b. Ensure BU compliance with Media Protection Policy; and
- c. Promote efforts within the BU to establish and maintain effective use of state information systems and assets.

5.4 BU CIO shall:

- a. Work with the BU Director to ensure the correct and thorough completion of BU Information Technology PSPs; and
- b. Ensure Media Protection PSPs are periodically reviewed and updated.

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 IT PSPs;
- b. Ensure the development and implementation of an adequate controls enforcing Media Protection PSPs for the BU;
- c. Request changes and/or exceptions to existing Media Protection PSPs from the State CISO; and
- d. Ensure all personnel understand their responsibilities with respect to protection of removable media in connection with state information systems and premises.

5.6 Supervisors of state employees and contractors shall:

- a. Ensure users are appropriately trained and educated on Media Protection Policies; and
- b. Monitor employee activities to ensure compliance.

5.7 Users of state information systems shall:

- a. Familiarize themselves with this policy and related PSPs; and
- b. Adhere to PSPs regarding protection of removable media in connection with state information systems and premises.

6. STATEWIDE POLICY

- 6.1 Media Access** - The BU shall restrict access to digital and non-digital media to authorized individuals. [NIST 800-53 MP-2] [HIPAA 164.308(a)(3)(ii)(A)] [PCI DSS 9.9] [IRS Pub 1075]
- 6.2 (P) Media Marking** - The BU shall mark, in accordance with BU policies and procedures, information system digital and non-digital media containing Confidential information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information, as well as exempt removable digital media from marking as long as the exempted items remain with a controlled environment. [NIST 800-53 MP-3] [PCI DSS 9.7.1] [IRS Pub 1075]
- 6.3 (P) Media Storage** - The BU shall physically control and securely store digital and non-digital media containing Confidential information within controlled areas. [NIST 800-53 MP-4] [ARS 39-101] [PCI DSS 9.6] [PCI DSS 9.9] [IRS Pub 1075]

- 6.4 (P) Media Inventories** - The BU shall maintain inventory logs of all digital media containing Confidential information and conduct inventories annually. [PCI DSS 9.9.1]
- 6.5 (P) Media Transport** - The BU shall protect and control digital and non-digital media containing Confidential information during transport outside controlled areas. [NIST 800-53 MP-5] [PCI DSS 9.7] [IRS Pub 1075]
- 6.5.1 (P) Cryptographic Protection** - The BU shall employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas. Cryptographic mechanisms must comply with System and Communication Protection Standard S8350. [NIST 800-53 MP-5(4)] [HIPAA 164.312(c)(2)] [IRS Pub 1075]
- 6.5.2 (P) Secure Delivery** - The BU shall send confidential digital and non-digital media by secured courier or other delivery method. [PCI DSS 9.7.2]
- 6.5.3 (P-HIPAA) Record of Movement** - The BU shall maintain a record, including the person(s) responsible, of the movements of hardware and digital media. [HIPAA 164.310(d)(2)(iii)]
- 6.5.3.1 (P) **Data Backup** - The BU shall create a retrievable, exact copy of Confidential data, when needed before movement of equipment. [HIPAA 164.310(d)(2)(iv)]
- 6.5.3.2 (P) **Backup Storage** - The BU shall store digital media backups in a secure location and review the location's security, at least annually. [PCI DSS 9.5]
- 6.5.4 (P) Management Approval** - The BU shall ensure management approves any media that is moved from a controlled area. [PCI DSS 9.8]
- 6.6 Media Sanitization** - The BU shall sanitize digital and non-digital information system media containing Confidential information prior to disposal, release of organizational control, or release for reuse using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250. [NIST 800-53 MP-6] [HIPAA 164.310(d)(2)(i)] [HIPAA 164.310(d)(2)(ii)] [IRS Pub 1075]
- 6.7 Media Use** - The BU shall restrict the use of [BU-specified type of digital media] on [BU-specified state information systems and/or system components]. [NIST 800-53 MP-7] [IRS Pub 1075]
- 6.7.1 (P) BU Restrictions** - The BU shall employ PSPs on the use of removable media in BU state information systems. [NIST 800-53 MP-7(1)] [HIPAA 164.310(d)(1)]
- 6.7.2 (P) Prohibition of Use without Known Owner** - The BU shall prohibit the use of removable media in BU state information systems when the media has no identifiable owner. [NIST 800-53 MP-7(2)] [IRS Pub 1075]

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

- 8.1** Statewide Standard S8250, Media Protection,
- 8.2** Statewide Standard S8350, System and Communication Protection
- 8.3** Statewide Policy Exception Procedure
- 8.4** NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.
- 8.5** HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006
- 8.6** Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.
- 8.7** IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
5/1/14	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director