



# STATEWIDE POLICY



State of Arizona

## STATEWIDE POLICY (8250): MEDIA PROTECTION

DOCUMENT NUMBER:	P8250
EFFECTIVE DATE:	January 16, 2024
REVISION:	4.0

### 1. AUTHORITY

---

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the BU 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 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. § 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

- 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, (Agency) 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 statewide information security PSPs throughout all state budget units (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 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 Information Security 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 agency systems and assets.

**5.5** BU CIO shall:

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

**5.6** 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 Information Security 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 agency systems and premises.

**5.7** Supervisors of agency employees and contractors shall:

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

**5.8** Users of agency systems shall:

- a. Familiarize themselves with this policy and related PSPs; and
- b. Adhere to PSPs regarding protection of removable media in connection with agency 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 9.6] [IRS Pub 1075]
- 6.2 (P) Media Marking** - The BU shall mark, in accordance with BU policies and procedures, 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 9.6.1] [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 9.5] [PCI DSS 9.7] [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 9.7.1]
- 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 9.6] [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 SC-28(1)] [HIPAA 164.312(c)(2)] [IRS Pub 1075]
- 6.5.2 (P-PHI) Media Transport Policies** - The BU shall implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Confidential information into and out of a protected facility, and the movement of these items within the facility. [HIPAA 164.310(d)(1)]
- 6.5.3 (P) Secure Delivery** - The BU shall send confidential digital and non-digital media by secured courier or other delivery method. [PCI DSS 9.6.2]
- 6.5.4 (P-PHI) 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)]
- 6.5.4.1 (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)]

**6.5.4.2 (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 9.5.1]

**6.5.5 (P) Management Approval** - The BU shall ensure management approves any media that is moved from a controlled area. [PCI DSS 9.6.3]

**6.6 Media Sanitization** - The BU shall sanitize digital and non-digital 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] [PCI DSS 9.8, 9.8.1, 9.8.2]

**6.6.1 Secure Storage** - Secure storage containers used for materials that are to be destroyed. [PCI DSS 9.8.1]

**6.6.2 (P-FTI) Verify Sanitization** - The BU shall review, approve, track, document, and verify media sanitization and disposal actions. [NIST 800-53 MP-6(1)] [IRS Pub 1075]

**6.7 Media Use** – The BU shall restrict the use of [BU-specified type of digital media] on [BU-specified agency systems and/or system components] and prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.. [NIST 800-53 MP-7] [IRS Pub 1075]

## 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 P8250 Media Protection

**8.2** Statewide Policy Exception Procedure

**8.3** Statewide Standard S8250, Media Protection

**8.4** System and Communication Protection, Standard S8350

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

**8.6** HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

- 8.7** Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.
- 8.8** IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

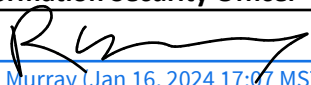
**9. ATTACHMENTS**

---

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	 <a href="#">Ryan Murray (Jan 16, 2024 17:07 MST)</a> Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer





# P8250\_Media\_Protection (1)

Final Audit Report

2024-01-17

Created:	2024-01-16
By:	Ed Yeargain (eyeargain@azdohs.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAU6wAjr_o1an_XduqUvtrJRtwfZ2Qv3_

## "P8250\_Media\_Protection (1)" History

-  Document created by Ed Yeargain (eyeargain@azdohs.gov)  
2024-01-16 - 11:46:37 PM GMT
-  Document emailed to Ryan Murray (rmurray@azdohs.gov) for signature  
2024-01-16 - 11:47:20 PM GMT
-  Document e-signed by Ryan Murray (rmurray@azdohs.gov)  
Signature Date: 2024-01-17 - 0:07:11 AM GMT - Time Source: server
-  Agreement completed.  
2024-01-17 - 0:07:11 AM GMT