ARIZONA STATEWIDE SECURITY STANDARDS	STATEWIDE STANDARD	State of Arizona

STANDARD 8250: MEDIA PROTECTION

DOCUMENT NUMBER:	**S8250**
EFFECTIVE DATE:	**JULY 1, 2015**
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 standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

3.1 Application to Budget Units (BUs) - This standard shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 Application to Systems - This standard shall apply to all state information systems. Standard statements preceded by "(P)" shall be required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

4. EXCEPTIONS

None.

5. ROLES AND RESPONSIBILITIES

a. 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).

b. 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.

c. 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.

d. 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 to reflect changes in requirements.

E. 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 CISCO; and

d. Ensure all personnel understand their responsibilities with respect to protection of removable media in connection with state information systems and premises.

F. 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.

G. Users of state information systems shall:

a. Familiarize themselves with this and related PSPs; and

b. Adhere to PSPs regarding protection of removable media in connection with state information systems and premises.

6. STATEWIDE STANDARD

6.1 Media Sanitization - The following standards are currently in place for media sanitization for any media installed, connected, or used within a state information system.

6.1.1 Sanitization Techniques - The following sanitization techniques may be applied to reissued, reused, or discarded media.

a. Clear Data - Overwriting of storage space on media with non-Confidential random data. This process includes overwriting of the logical storage space and all other addressable locations.

b. Purge Data - Rendering sanitized data unrecoverable by laboratory attack methods. Purge techniques include degaussing and firmware Secure Erase command (ATA drives).

c. Destroy Media - Action taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.

6.1.2 Sanitization Methods - The following sanitization methods may be applied to media according to the minimum sanitization standards in Table 1.1.

a. Overwrite: Use of approved software to perform an overwrite to every accessible data location on the media.

b. Overwrite Long-term: Use of approved software to perform an overwrite to every accessible data location on the media and ensure that overwrite data remains in memory longer than the previous data resided.

c. UV Erase: Use of ultraviolet light directed onto the die of an EPROM to dissipate the stored charge on the floating gate. EPROMs shall be removed from equipment for proper erasure.

d. Secure Erase: Use of the firmware-based overwriting technology. This process is a command defined in the ANSI ATA and SCSI disk drives interface specifications and runs inside the drive hardware. Secure Erase completes in about 1/8 the time of a block eraser.

e. Scissor Cut: Use of scissors or other cutting device to cut the storage device at 45 degree angle into several pieces.

f. Cross Cut Shred: Use of cross cut shredder to reduce hard copy or device into pieces 5mm or smaller

g. Strip Shred: Use of strip shredder to cut device in strips no wider than 2mm.

h. Full Chip Purge: Electronically erase contents of Electronically Alterable Programmable Read Only Memory (EAPROM) per manufacturer's data sheets.

i. Manufacturer's Reset: Perform a full manufacturer's reset to reset the copy machine to its factory default settings. Contact manufacturer for proper procedures.

j. Remove Power: Power off, remove battery (if battery backed). This technique works on RAM or volatile memory.

k. Grind: Use of a grinder or sander to remove information bearing layers (CDs only).

l. Emboss/Knurl: Use of Embosser or Knurler to cut a pattern into the material thus destroying all data layers.

m. Degauss: Generation of a strong magnetic force sufficient to reduce remnant magnetic fields to near zero. The ability of magnetic media to hold a charge is referred to as coercivity. The magnetic field produced by a degausser is measured in Oersted. Degausser shall be of sufficient strength to overcome coercivity of the media and shall be used in accordance with manufacturer directions.

n. Raise Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure.

o. Incineration: Use of licensed incinerator to reduce to white ash

p. Disintegrate: Use of equipment to break device into particles of 2mm or less.

q. Pulverize: Use of equipment to grind into a powder or dust.

r. Chemical Reaction:Immersion of film in household bleach.

6.1.3 (P) Sanitization through Approved Devices - Sanitization techniques shall be performed using an approved product or a licensed operator. The following references shall be used to determine the approval of products:

a. Overwrite: Overwriting or wiping shall be performed by a product on the National Information Assurance Partnership, Common Criteria Evaluation & Validation Scheme's Product Compliant List.

b. Grind: Grinding shall be performed by a product listed in NSA/CSS Specification 04-02, Optical Media Destruction Devices

c. Degaussers: Degaussing of electronic magnetic media shall be performed by a product on the National Security Agencies Evaluated Products List (NSA's EPL)

d. Shred: Strip and Cross Cut shredding shall be performed by a product listed in NSA/CSS Specification 02-01, High Security Crosscut Paper Shredders

e. Disintegration: Disintegration shall be performed by a product listed in NSA/CSS Specification 02-02, High Security Disintegrators

6.1.4 Sanitization Process Diagram - BUs shall use the figure below and the information in this standard to determine the process for required for media sanitization. Sanitization process is based on the sensitivity of the data and the control of the media.

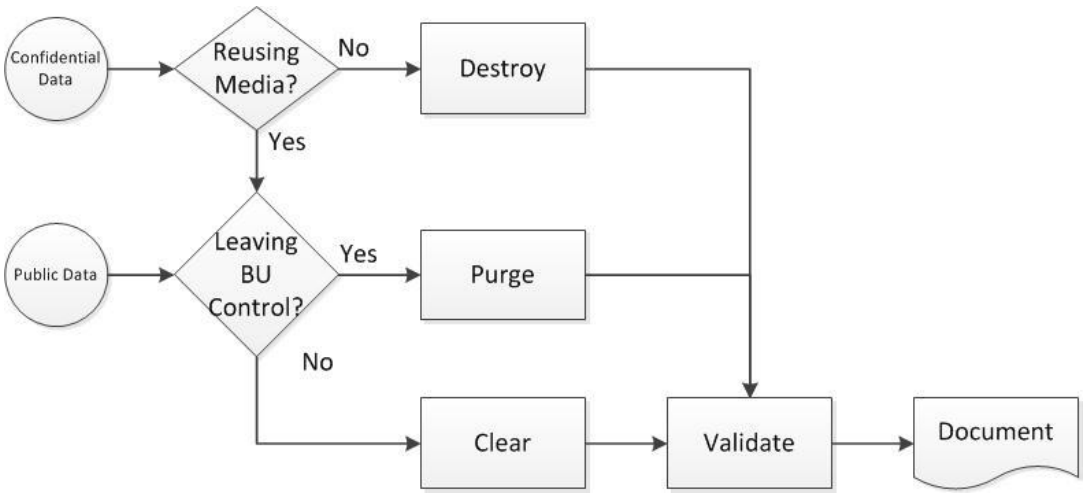

Figure 1.1. Data Sanitization and Disposition Process. *Sanitization process is based on the sensitivity of the data and the control of the media.*

6.1.5 Sanitization Process - All media installed, connected, or used within a state information system shall follow the sanitization process below:

a. **(P) Confidential Data Sanitization (Destroy, Purge or Clear)** - Media not intended for reuse shall be destroyed; Media intended for reuse and leaving control of the BU shall be purged; media intended for reuse but not leaving control of the BU shall be cleared.

b. **Public Data Sanitization (Purge or Clear)** - Media leaving control of the BU shall be purged; media intended for reuse but not leaving control of the BU shall be cleared.

6.1.6 Sanitization Verification Process - The BU shall verify the sanitization and disposal process through:

a. Testing a representative sample of the media; and

b. Utilizing personnel without a stake in any part of the process to verify.

6.1.6.1 **Equipment Calibration** - If the BU utilizes sanitization tools (e.g., a degausser) to perform sanitization techniques these tools shall be:

a. Used in accordance with the manufacturer's instructions;

b. Calibrated, tested, and maintained according to manufacturer's instructions.

6.1.6.2 **Personnel Training** - If the BU utilizes sanitization tools (e.g., a degausser) to perform sanitization techniques:

a. The personnel conducting the sanitization shall be competent to perform the sanitization functions; and

b. The equipment shall be used in accordance with the manufacturer's instructions.

6.1.7 Sanitization Documentation Process. The BU shall maintain a record of its sanitization. Sanitization documentation shall include the elements below.

a. The media sanitized;

b. Date sanitization occurred;

c. Method of sanitization; and

d. Final disposition of data.

***Note**: A sample Sanitization Document Form is attached as Appendix A. Media not containing Confidential data (e.g., public data only) may be considered a consumable or perishable item and not be required to undergo sanitization documentation.*

6.1.8 Media and Document Destruction Services - If the BU has contracted with a service to provide purge or destruction services the media shall be kept securely until purge or destruction is accomplished.

6.1.9 Minimum Sanitization Standards for Media Containing Data - The tables below shall be used to determine the minimum sanitization standards for different types of media.

Sanitization Standards	Clear	Purge	Destroy
Hard Copy Storages			
Paper	N/A	N/A	• Shred
Microforms	N/A	N/A	• Incinerate • Chemical Reaction
Hand-Held Devices			
Cell Phones	• Manually delete all information, such as calls made, phone numbers and • Manufacturer's Reset		• Shred • Disintegrate • Pulverize • Incinerate
Networking Devices			
Routers	Manufacturer's Reset		• Shred • Disintegrate • Pulverize • Incinerate
Equipment			
Copy Machines Fax Machines	Manufacturer's Reset		• Shred • Disintegrate • Pulverize • Incinerate
Magnetic Disks			
Floppy Disks	Overwrite	Degauss	• Incinerate • Shred
ATA Hard Drives (HD) and USB Removable Media with HD	Overwrite	• Secure Erase1. • Degauss Hard Drive. • Degauss Wand disassemble hard drive platters	• Shred • Disintegrate • Pulverize • Incinerate
USB Removable Media	Overwrite		
Zip Disks	Overwrite	Degauss	• Incinerate • Shred
SCSI Drives	Overwrite	Degauss	• Shred • Disintegrate • Pulverize • Incinerate
Magnetic Tapes			
Reel and Cassette Format Magnetic Tapes	• Overwrite • Degauss	Degauss	• Shred • Incinerate

[1] The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site.

Sanitization Standards	Clear	Purge	Destroy
Optical Disks			
CDs	N/A - Destroy		• Grind • Incinerate • Shred
DVDs			
Memory			
Compact Flash Drives, SD Cards	Overwrite	N/A - Destroy	• Shred • Disintegrate • Pulverize • Incinerate
DRAM	Remove Power	N/A – Destroy	• Shred • Disintegrate • Pulverize
EAPROM	Full chip purge		• Shred • Disintegrate • Pulverize
EEPROM	Overwrite		• Shred • Disintegrate • Pulverize • Incinerate
EPROM	• UV Erase • Overwrite		
FPGA Devices (Non-Volatile)	Overwrite		• Shred • Disintegrate • Pulverize
FPGA Devices (Volatile)	Remove Power		
Flash Cards	Overwrite		
Flash EPROM	Full Chip Purge	• Overwrite • Full Chip Purge	• Shred • Disintegrate • Pulverize • Incinerate
Magnetic Bubble Memory	Overwrite	• Degauss (remove shielding) • Raise Magnetic Bias Field	• Shred • Disintegrate • Pulverize
Magnetic Core Memory	• Overwrite • Degauss (remove shielding)		
Non Volatile RAM	• Overwrite Long-term • Remove Power		
PC Cards / PCMCIA Cards	N/A - Destroy		• Incinerate
PROM	N/A - Destroy		
RAM	Remove Power		• Shred • Disintegrate • Pulverize
ROM	N/A - Destroy		• Shred • Disintegrate • Incinerate
USB Removable Media w/o HD	Overwrite		

Sanitization Standards	Clear	Purge	Destroy
Smart Cards	N/A - Destroy		• Scissor Cut • Strip Shred • Shred
Tokens	N/A - Destroy		• Disintegrate • Incinerate
Magnetic Cards			
Magnetic Cards	Overwrite	Degauss	• Shred • Incinerate

Table 1.1. Sanitization Procedures. *Sanitization procedures for media types and sanitization method (e.g., Clear, Purge, Destroy).*

6.2 **Media Under BU Control** - Media under the control of the BU is subject to fewer threats and can protected more easily. For the purposes of media sanitization requirements the following definitions of BU control shall be applied.

6.2.1 **Under BU Control** - Media is considered under BU control if:

a. The media is currently being used within the BU environment;

b. The media is currently being used in a virtual office environment supporting the BU mission;

c. The media has been turned over for maintenance AND the maintenance provider specifically provides for the confidentiality of the information; or

d. Maintenance is being performed on the BU's site, under the BU's supervision, OR by a maintenance provider.

6.2.2 **Not Under BU Control** - Media is not considered under BU control if the media has been exchanged for warranty, cost rebate, or other purposes and the media will not be returned to the BU.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-88, September 2006.

8.2 DoD 5220.22-M. National Industrial Security Program Operating Manual (NISPOM) January 1995. U.S. Government Printing Office ISBN0-16-045560-X

8.3 Evaluated Products List – Degausser, National Security Agency, May 16, 2012, http://www.nsa.gov/ia/_files/government/MDG/EPL_Degausser25June2012.pdf.

8.4 Evaluated Products List for High Security Crosscut Paper Shredders, National Security Agency, April 30, 2009. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-02-01.pdf

8.5 NSA/CSS Evaluated Products List for Optical Media Destruction Devices, National Security Agency, September 25, 2009, http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_EPL_04-02-H.pdf

- NSA/CSS Storage Device Declassification Manual, 9-12.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director