STATE of ARIZONA

Government Information Technology Agency	**Statewide STANDARD** P800-S880 Rev 2.0	**TITLE: Media Sanitizing/Disposal** **Effective Date: October 10, 2008**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) (A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to identify the proper requirements for media sanitizing and the disposal of IT devices (servers, storage, and clients), network components, operating systems, application software, mobile devices, and storage media, to prevent the unauthorized use or misuse of the state's information assets.

3. SCOPE

This applies to all budget units. A budget unit is defined as a department, commission, board, institution or other agency of the state organization 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).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

The following standards shall be followed in protecting the information assets of the state when a budget unit decides to redeploy or dispose of Information Technology assets with memory and disk storage capabilities. This also includes network components, operating systems, application software, mobile devices, and storage media:

4.1. ARCHIVING INFORMATION RECORDS: Budget units shall perform final disposition of public/official records maintained on all IT devices with the Arizona State Library, Archives, and Public Records (ASLAPR) A.R.S. § 41-1339. When final disposition has been completed, the process of removing data can then be performed and the IT devices can either be redeployed internally, or redeployed to other budget unit(s), or disposed of through State Surplus.

4.2. DATA SANITIZATION: All budget units shall perform data sanitization for removing data/files from storage media. Deleting or clearing data/files removes only information from a user's directory and does not physically remove the data from disk storage. Even reformatting a storage disk does not completely

remove data/files since it can be retrieved through the use of sophisticated utilities. Therefore, budget units shall perform one of the sanitization methods below when redeploying or disposing of IT assets:

4.2.1. DEGAUSSING: This process magnetically erases data from magnetic media and hard drive. It renders any previously stored data completely unreadable and unrecoverable.

4.2.2. OVERWRITING: This process is an effective method for sanitizing data and uses a program to overwrite (ones, zeros or a combination of both) onto existing data. This method requires a minimum of three overwrites for complete sanitization.

4.2.3. DESTROYING: This process is the most effective method for data sanitation, since the storage media is completely destroyed either through shredding, disintegration, incineration, pulverizing, or melting as a best practice.

4.3. REMOVAL OF SENSITIVE DATA: Prior to the off-site repair of IT devices, network components, operating system or application software, or storage media, the budget unit shall remove all sensitive (confidential and/or personal information) data from the IT devices, network components, operating systems, application software, and storage media. In the event that the storage media is unable to be repaired, the budget unit shall have it destroyed (disintegrate, incinerate, pulverize, shred or melt).

4.4. ASSURANCE OF SENSITIVE DATA REMOVAL: The budget unit shall verify that the storage media no longer contains readable or sensitive data, as applicable. Where practical and feasible, separation of duties should be employed for sanitization removal and verification procedures.

4.5. AUTHORIZED PERSONNEL: Only authorized personnel shall be used to effect the sanitization of data from any IT devices.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."

6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."
6.11. A. R. S. § 44-7041, "Governmental Electronic Records."
6.12. Arizona Administrative Code, Title 2, Chapter 7, "Department of Administration Finance Division, Purchasing Office."
6.13. Arizona Administrative Code, Title 2, Chapter 10, "Department of Administration Risk Management Section."
6.14. Arizona Administrative Code, Title 2, Chapter 18, "Government Information Technology Agency."
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P800, IT Security.
6.17. State of Arizona Target Security Architecture, http://www.azgita.gov/enterprise_architecture.

7. ATTACHMENTS

None.