Disposal of Information Technology Assets Directive
Arizona Department of Administration Surplus Property Management Office

Authority: A.A.C. R2-15-303

Purpose: To provide minimum standards for the removal of data from Information Technology Assets and Removable Storage Media sent to or through the ADOA Surplus Property Management Office

Effective Date: Update Effective May 18th, 2010

Termination Date: This directive shall remain in effect until rescinded or amended in writing by the ADOA SPMO.

Applicability: All Information Technology Assets and Removable Storage Media processed to or through the ADOA Surplus Property Management Office.

Definitions:

ADOA - Arizona Department of Administration

Data Destruction - The process of removing programs or data files on Devices or Removable Storage Media in a manner that gives assurance that the information cannot be recovered.

Device - Includes, but is not limited to: personal computers with hard drives; servers with hard drives; digital copy machines; printers; scanners; fax machines; smart and cell phones; other assets with hard drives or loose / unattached hard drives.

Information Technology Asset - Any Device or component of a Device that can store information in an electronic format including Removable Storage Media.

Removable Storage Media - Includes, but is not limited to: magnetic tapes, CD's; DVD's; Zip media; Flash media; USB Flash Drives; SIMS Chips; etc.

SPMO - ADOA Surplus Property Management Office

Physical Destruction – To disintegrate, incinerate, pulverize, shred, or melt: the Device; component thereof; or Removable Storage Media.

SP152 Certification of Data Destruction – SPMO supplied form on which an agency certifies that it has complied with the conditions set forth in this directive for the disposal of Information Technology Assets.

Note: These definitions apply only in the context of this document and when used in the form shown, the definitions above shall apply.

Policy

It is the policy of the ADOA SPMO that all Information Technology Assets that have the capacity for electronic storage of data or information shall be subjected to Data Destruction by sanitizing / scrubbing of data and or programs prior to being surplused, transferred, traded-in, or disposed of to or through the ADOA SPMO. This directive sets forth the minimum requirements for the level of Data Destruction that must be accomplished. This policy in no way supersedes the P800-S880 Rev 2.0 Security Standard established by the Government Information Technology Agency (GITA). All agencies should be familiar with the applicable GITA Standards and comply accordingly.

1.0 General Standards

1.1 Before an Information Technology Asset is surplused, transferred, traded-in, disposed of, or the hard drive within the Asset is replaced, Data Destruction must be completed and all data or program files on any storage media must be completely removed or otherwise made unrecoverable in accordance with this Directive unless there is specific intent to transfer the particular software or data to the purchaser / recipient.

1.2 Hard drives of surplus Devices shall be securely erased or destroyed within 30 days after replacement and always prior to release outside the owning agency.

1.3 Whenever licensed software is resident on any Information Technology Asset being surplused, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement must be followed. In most cases, the software must be totally removed from the Information Technology Asset.

1.4 After removal of data and / or programs from the Asset is complete, the process must be certified, as specified in this directive and a record maintained as specified by the disposing agency's records retention schedule.

1.5 Each agency shall test for compliance with this directive and keep a record of testing.

2.0 Methods of Removing Data from Information Technology Assets

The following section outlines the acceptable methods and procedures for removing data from Devices and Removable Storage Media. Data Destruction must be performed to ensure that information is removed in a manner that gives assurance that the information cannot be recovered. The method used for removal of data depends on the operability of the Device.

2.1 Operable Desktop Computers; Laptop Computers; Loose Hard Drives;

Overwriting is accepted as a method of Data Destruction from operable desktop personal computers, lap top computers, and loose hard drives. Overwriting of data means replacing the previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable.

2.1.1 Overwriting Standards

2.1.1.a The Data must be properly overwritten with a pattern. SPMO has adopted the Department of Defense standard (DoD 5220.22-M) which requires overwriting with a pattern, then its complement, and finally with a random pattern of 1's and 0's.

2.1.1.b Removal of data is not complete until at least three (3) overwrite passes and a verification pass is complete.

2.1.1.c The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, any unused disk space and of every addressable bit location on the entire hard disk medium.

2.1.1.d The software must have a method to verify that all data has been removed. Approved software applications are listed in Section 4.0 of this document.

2.1.1.e To assist agencies with this directive, the SPMO has obtained a license from one of the approved software vendors and will make overwrite software available to agencies.

2.1.1.f Upon completion of the overwrite and verification process, the agency shall certify on SPMO form SP152 *Certification of Data Destruction* that the overwrite and verification was completed.

2.1.1.g A completed, signed and dated certification (form SP152) shall be attached to the Surplus Property Disposal Request (form SP101) for any action to or through the SPMO which includes a covered Information Technology Asset.

2.2 In-operable Desktop Personal Computers; Laptop Computers; and Loose Hard Drives

In-operable Information Technology Assets may include, but is not limited to: Devices or components of Devices in in-operable condition. The process for accomplishing Data Destruction for these Devices is described below.

2.2.1 In-operable Standards

2.2.1.a Remove the hard drive from the Device.

2.2.1.b Drill three holes no smaller than 3/8's of an inch through the drive platens from top to bottom in different areas of the drive.

2.2.1.c After drilling through the drive has been completed, turn the drive into ADOA SPMO for final Physical Destruction.

2.2.1.d If the drive was removed from a Desktop PC or Laptop being turned in to the SPMO, note on the SP101 that the hard drive was removed and drilled. The accompanying SP152 *Certification of Data Destruction* still needs to be completed and note made when and by whom drilling was performed.

2.3 Removable Storage Media

Removable Storage Media such as Magnetic Tapes, CD's DVD's shall be subject to either degaussing or Physical Destruction. Degaussing is a process whereby the magnetic media is erased. **Please note that extreme care should be used when using degaussing equipment since this equipment can cause extreme damage to nearby telephones, monitors, personal computers and other electronic equipment. Appropriate warnings should also be posted at entrances to the workplace cautioning that degaussing equipment is in use.**

2.3.1 Degaussing Standards

2.3.1.a Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

2.3.1.b Shielding materials (cabinets, or mounting brackets), which may interfere with the degausser's magnetic field must be removed from the media before degaussing.

2.3.1.c Media must be placed in a horizontal direction during the degaussing process.

2.3.1.d Degaussing efforts must be periodically audited to detect equipment or procedural failures.

2.3.2 Physical Destruction Standards for Removable Electronic Media

2.3.2a Removable Electronic Media shall be shredded, mutilated, or pulverized to the extent that precludes any possible further use of the Media.

2.4 Servers and NAS / SAN Hardware

Data Destruction on Hard Drives from SAN's or Servers shall be accomplished in one of three ways.

2.4.1 Hard Drives in a SAN or Server may be removed from the Devise, individually overwritten to the same level as described in Section 2.1 of this Directive and returned to the SAN or Server.

2.4.2 Drives may be destroyed by drilling as described in Section 2.2 of this Directive and turned into the SPMO as loose hard drives for final Physical Destruction.

2.4.3 Drives may be destroyed by shredding using the services of a third party certified to perform this type of activity. If an agency utilizes this method, a written certification provided by the third part certifying the drives have been destroyed must accompany the SP152 Certification of Data Destruction when the Device is sent to Surplus.

2.5 Copiers, Printers and Multifunction devices with Hard Drives or other Storage Media

2.5.1.a Overwriting is accepted as a method of Data Destruction from operable from Copiers and other Multifunction devices with hard drives or other storage media. Overwriting shall be accomplished to the level specified in Section 2.1.1 of this Directive.

2.5.1.b Use of the Device manufacturers overwrite software is acceptable provided the software is certified to accomplish the overwrite to the standards outlined in Section 2.1.2 of this directive.

2.5.1.c For inoperable Copies or other multifunction devices with hard drives or other storage media, the drives and media shall be removed from the device and the drive destroyed to the level specified in 2.2 of this directive.

2.5.1.d Upon completion of the data destruction and verification process, the agency shall certify on SPMO form SP152 *Certification of Data Destruction* that the overwrite and verification was completed.

2.5.1.e A completed, signed and dated certification (form SP152) shall be attached to the Surplus Property Disposal Request (form SP101) for any action to or through the SPMO which includes a covered Information Technology Asset.

3.0 Unacceptable methods of accomplishing Data Destruction

Clearing Data (deleting files) is NOT ACCEPTABLE. Clearing data (deleting files) removes information from Information Technology Assets in a manner that renders it unreadable unless utility software or techniques are used to recover the cleared media. However, because the clearing process does not prevent the data from being recovered by technical means, it is not an acceptable method of removing data from agency owned Devices or Removable Storage Media.

Under no circumstances should Hard Drives or other Removable Media including flash storage, USB drives, SD drives or other memory containing any information be thrown into the garbage, recycling or other trash receptacles. This method of disposal is not secure and could cause a breach of data security.

4.0 Acceptable Software Overwriting Applications

- Wipe Drive by Access Data inc. http://www.accessdata.com/products.htm
- Darik's Boot and Nuke "DBAN" share ware product http://dban.sourceforge.net/

5.0 Verification of Data Destruction

There are a number of freeware or low cost disk recovery utilities which can be used to verify Data Destruction has been accomplished. It is highly recommended agencies obtain this type of software and verify Data Destruction has been performed and incorporate this process into their Data Destruction procedures.

6.0 Additional Information or Questions

If you agency requires further information, has questions or suggestions to improve this directive, please contact the ADOA Surplus Property Management Office at (602) 542 5701.