STATE OF ALABAMA

Information Technology Standard

STANDARD 681S3-00: MEDIA SANITIZATION

A key element of information security is confidentiality, protecting data stored on digital and non-digital media from unauthorized disclosure throughout the system life cycle. Legacy data remaining on storage media poses significant security vulnerability and is an organizational liability if the data is compromised or otherwise disclosed. When storage media are transferred, become obsolete, or are no longer usable as a result of damage, it is important to ensure that residual magnetic, optical, or electrical representation of data that has been deleted is no longer recoverable. Sanitization is the process of removing data from storage media, such that there is reasonable assurance, in proportion to the sensitivity of the data, that the data may not be retrieved and reconstructed. Once the media is sanitized, it should be impossible or impractical to retrieve the data.

OBJECTIVE:

Define requirements for sanitization of stored data assets that provide an appropriate level of security (in accordance with State IT Policy 681: Information Protection) to State of Alabama information.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

The following State of Alabama requirements are based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-88: Guidelines for Media Sanitization.

Storage media covered by these requirements includes but is not limited to paper and microforms, hand-held devices (cell phones, personal digital assistants, palm devices), networking devices, floppies, hard drives, USB removable media with or without hard drives (including pen drives, thumb drives, flash drives, memory sticks), ZIP disks, magnetic tapes, optical disks, and memory.

SANITIZATION REQUIREMENTS

Prior to reuse, all electronic media (includes storage devices, memory, buffer, or other reusable memory) shall be cleared to effectively deny access to previously stored information.

All electronic media shall be purged prior to reuse in an environment that does not provide the same or higher level of protection for the data that was on the media before purging.

Prior to disposal, all electronic media that have reached the end of their operational life shall be purged in accordance with this standard.

All printed and other non-rewritable media (e.g., CD/DVD, microform, Smart Card, ROM), when no longer required to be maintained, shall be destroyed in accordance with this standard and organizational procedures.

SANITIZATION METHODS

There are several accepted methods for sanitizing media including overwriting, degaussing, and destruction. The cost and benefit of a media sanitization method should be understood prior to a final decision on which method to use.

Overwriting:

Use software or hardware products to overwrite storage space on the media with non-sensitive data. This process shall include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) to be erased or deleted but also the entire media, including all addressable locations. The security goal of the overwriting process is to replace sensitive data with non-sensitive random data. Media shall be overwritten a minimum of three times using a method based on the media type. Overwriting cannot be used for media that are damaged or not rewriteable. The media capacity may also influence whether overwriting is a suitable sanitization method.

Degaussing:

A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussing, also called demagnetizing, can be an effective method for sanitizing damaged media, for sanitizing media with exceptionally large storage capacities, or for quickly sanitizing diskettes (although it may not be cost effective to degauss inexpensive media like diskettes). Degaussing is not effective for sanitizing nonmagnetic media, such as optical media. Degaussing current generation hard drives (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable.

Destruction:

Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverization, and shredding, depending on the media type. Physical destruction may be the only appropriate sanitization method for optical media, such as CD-ROM (read only) and Write-Once Read-Many (WORM) media.

Disintegration, pulverization, melting, and incineration shall be conducted at a metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

Shredding can be used to destroy paper and some flexible media such as CDs and magnetic cards. The shred size of the refuse shall be small enough that there is reasonable assurance in proportion to the sensitivity of the data that the data cannot be reconstructed.

Memory Sanitization:

Volatile memory, such as RAM chips, requires power to maintain its content. Removing electrical power from the chip will erase or sanitize its contents. Nonvolatile memory, such as forms of Programmable Read-Only Memory (PROM) flash memory, maintain their contents permanently or until reprogrammed. Sanitization methods vary for specific forms of PROM (see table).

The table below describes several approved methods of media sanitization based on the media type. Select the method that best mitigates the risk of unauthorized disclosure of the information on the media.

Table: Media Sanitization Methods

Media Type	Clear	Purge	Physical Destruction
Hard Copy Storages			
Paper	See Physical Destruction.	See Physical Destruction.	Shred: Destroy paper using cross cut shredders which produce particles that are no greater than 1 x 5 millimeters in size. Pulverize/Disintegrate: Pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen.
Microforms	See Physical Destruction.	See Physical Destruction.	Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.
Hand-Held Devices			
Cell Phones	Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. ** Contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning cell phones in a licensed incinerator.
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's reset to reset the PDA to factory state. ** Contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Pulverize. Incinerate by burning the PDA in a licensed incinerator.
Networking Devices			
Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings. ** Contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate. Incinerate routers by burning the routers in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
Equipment			
Copy Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings. ** Contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.
Fax Machines	Perform a full manufacturer's reset to reset the fax machine to its factory default settings. ** Contact the manufacturer for proper sanitization procedures.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.
Magnetic Disks			
Floppies	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Degauss in a NSA/CSS-approved degausser.	Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator. Shred.
ATA Hard Drives	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Purge using Secure Erase (see Definitions). Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. Purge media by using organization-approved and validated purge technologies/tools.	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Purge using Secure Erase (see Definitions). Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. Purge media by using organization-approved and validated purge technologies/tools.	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
Zip Disks	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Degauss using a NSA/CSS-approved degausser.	Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. Shred.
SCSI Drives	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Magnetic Tapes			
Reel and Cassette Format Magnetic Tapes	Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded confidential or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.	Degauss using an NSA/CSS-approved degausser. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.	Incinerate by burning the tapes in a licensed incinerator. Shred. Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.
Optical Disks			
CDs / DVDs	See Physical Destruction.	See Physical Destruction.	Removing the Information bearing layers of CD/DVD media using a commercial optical disk grinding device. Incinerate optical disk media (reduce to ash) using a licensed facility. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2).

Media Type	Clear	Purge	Physical Destruction
Memory			
Compact Flash Drives, SD (Secure Digital) Memory Cards	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	See Physical Destruction.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's instructions.	Same as Clear.	Shred Disintegrate Pulverize
Electronically Erasable PROM (EEPROM)	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
Erasable Programmable ROM (EPROM)	Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time require-ment by a factor of 3. Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Field Programmable Gate Array (FPGA) Devices (Volatile)	Clear functioning FPGA by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
Flash Cards	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Flash EPROM (FEPROM)	Perform a full chip purge per manufacturer's instructions.	Overwrite media by using organization-approved and validated overwriting technologies/methods/tools. Perform a full chip purge as per manufacturer's instructions.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
Magnetic Bubble Memory	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing. 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. Specific technical guidance should be obtained from the bubble memory manufacturer before attempting this procedure.	Shred. Disintegrate. Pulverize. When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Magnetic Core Memory	Overwrite media by using organization-approved and validated overwriting technologies/methods/tools Degauss in an NSA/CSS-approved degausser.	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure performance and should be considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing.	Shred. Disintegrate. Pulverize. When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance.
Non Volatile RAM (NOVRAM)	Overwrite media by using organization-approved and validated overwriting technologies/methods/tools Each overwrite must reside in memory for a period longer than the data resided. Remove all power to include battery power.	Same as Clear.	Shred. Disintegrate. Pulverize.

Media Type	Clear	Purge	Physical Destruction
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator.
RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
ROM	See Physical Destruction.	See Physical Destruction.	Shred. Disintegrate. Pulverize.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Smart Cards	See Physical Destruction.	See Physical Destruction.	For smart cards and data storage tokens in credit card form, cut or crush the smart card's internal memory chip using metals snips, scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust packages) that are not capable of being shredded should instead be destroyed via disintegration to 2 mm size particles or incinerated.
Magnetic Cards			
Magnetic Cards	Overwrite media by using organization-approved and validated overwriting technologies/methods/ tools	Degauss in an NSA/CSS-approved degausser.	Shred. Incinerate. Burn magnetic cards in a licensed incinerator.

SANITIZATION DEVICES

There are many different tools, methods, and technologies available for media sanitization, and organizations may select from commercially available technologies provided that the selection meets the requirements of this standard.

The National Security Agency (NSA) evaluates media sanitization devices (including degaussers, disintegrators, shredders, etc.) and publishes evaluated products lists of the devices that meet NSA-specific performance requirements. NSA-evaluated products lists can be found here:

http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

SANITIZATION PROCESS

1. Determine the sensitivity of the data stored on the media.
2. Determine whether the media will be reused in an environment that provides an acceptable level of protection for the data that was on the media before sanitization to determine whether to clear, purge, or destroy the media.
3. Determine the type (e.g., optical non-rewritable, magnetic, volatile, nonvolatile) and size (e.g., megabyte, gigabyte, and terabyte) of storage media to be sanitized.
4. Select the sanitization method appropriate for the media type, data sensitivity, and reuse environment.
5. Determine whether sanitization will be conducted within the organization or outsourced. Determination will depend in part on whether the organization has the appropriate sanitization devices.
6. Conduct sanitization; validate to ensure sanitization was successful.
7. Document the results to record what media was sanitized, when, how, and the final disposition of the media to ensure proper accountability of equipment and inventory control.

SANITIZATION PROCEDURES

Agency Heads, IT Managers, and/or Information Security Officers shall:

1. Establish media sanitization procedures addressing both the reuse and disposal of data storage media containing Confidential, Sensitive, or Internal information. Procedures shall address all media types including but not limited to those listed herein. Procedures shall also address repair and replacement issues, offsite maintenance, and end-of-life disposal of State and agency IT resources.
2. Establish procedures to ensure that all non-public information in printed form is disposed of in accordance with this standard.
3. Ensure that appropriate sanitization devices such as degaussers and paper and digital media shredders are available (internally or outsourced).
4. Periodically test sanitization devices and procedures to ensure correct operation.
5. Ensure all personnel are trained in their responsibilities and on the proper use of sanitization devices.

ADDITIONAL INFORMATION:

Information Technology Policy 681: Information Protection
http://cybersecurity.alabama.gov/documents/Policy_681_Information_Protection.pdf

Information Technology Standard 681S1: Information Protection
http://cybersecurity.alabama.gov/documents/Standard_681S1_Information_Protection.pdf

Information Technology Standard 681S2: Protecting Personally Identifiable Information
http://cybersecurity.alabama.gov/documents/Standard_681S2_Protecting_PII.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
680-01S4	10/15/2007	Original document
681S3-00	09/01/2011	Replaces Standard 680-01S4 (number and format change only)