NSA/CSS STORAGE DEVICE SANITIZATION MANUAL

PURPOSE AND SCOPE

This manual provides guidance for sanitization of information system (IS) storage devices for disposal or recycling in accordance with NSA/CSS Policy Statement 9-12, "NSA/CSS Storage Device Sanitization" (Reference a). Information stored on these devices may range from UNCLASSIFIED to TOP SECRET and may include compartmented, sensitive, or limited-distribution material. This manual also provides information on how to obtain NSA/CSS Evaluated Products Lists and hard disk drive crushers that meet NSA/CSS specifications.

This manual applies to all NSA/CSS elements and pertains to all IS storage devices utilized by NSA/CSS elements, contractors, and personnel.

JOHN TAFLAN
Associate Director for
Installations and Logistics

Endorsed by
Associate Director for Policy

DISTRIBUTION:
LL-CSDSR
DJ1

NSA/CSS Policy Manual 9-12 is approved for public release.
P134 (Vital Records)

This Policy Manual 9-12 supersedes NSA/CSS Policy Manual 9-12 dated 13 March 2006. The Chief, Policy approved an administrative update on 19 December 2017 to update organizational designators for NSA21, repair broken links, and make other administrative changes. OPI: Information Assurance Standards Center for Storage Device Sanitization Research, Y2D123, 301-688-1031, 977-7113s.
# TABLE OF CONTENTS

Purpose and Scope ................................................................................................................. 1

Procedures ............................................................................................................................... 4
  Magnetic Storage Devices ................................................................................................. 4
  Optical Storage Devices ................................................................................................. 6
  Solid State Storage Devices ......................................................................................... 6
  Hard Copy Storage Devices ......................................................................................... 7

Responsibilities ..................................................................................................................... 8

References .............................................................................................................................. 9

Definitions .............................................................................................................................. 9
PROCEDURES

1. Guidance for the sanitization and release of IS storage devices not covered by this document may be obtained by submitting all pertinent information to NSA/CSS (Attention: Y2D123 Information Assurance Center for Storage Device Sanitization Research, 301-688-1031, csdsr@nsa.gov).

MAGNETIC STORAGE DEVICES

2. Magnetic Tapes
   a. Sanitization: Sanitize magnetic tapes using one of the following procedures. Remove all labels or markings that indicate previous use or classification.
      
      1) **Degaussing:** Degauss using an NSA/CSS evaluated degauss; see Reference b.

      2) Incineration: Material must be reduced to ash.

   b. **Declassification:** Declassify magnetic tapes only after approved verification and review procedures are completed per Reference c.

   c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified magnetic tapes may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed per Reference c.

3. Magnetic Disks: Magnetic disks include hard disk drives and diskettes.

   a. Hard Disk Drives
      
      1) Sanitization: Sanitize hard disk drives using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

      a) Automatic Degausser: Degauss using an NSA/CSS evaluated degausser; see Reference b. It is highly recommended to physically damage the hard disk drive by deforming the internal platters prior to release by any means or by using a hard disk drive crusher (contact the Center for Storage Device Sanitization Research for further information on hard disk drive crushers).

      b) Degaussing Wand: Sanitize hard disk drives by disassembling the device and erasing all surfaces of the enclosed platters with an NSA/CSS evaluated hand-held degaussing wand; see Reference b. It is
highly recommended to physically damage the hard disk drive by
deforming the internal platters prior to release by any means or by using a
hard disk drive crusher (contact the Center for Storage Device Sanitization
Research for further information on hard disk drive crushers).

c) Disintegration: Disintegrate into particles that are nominally 2
millimeter edge length in size. It is highly recommended to disintegrate
hard disk drive storage devices in bulk lots with other storage devices.

    d) Incineration: Internal platter coating must be reduced to ash
and/or internal platters must be physically deformed from heating.

2) Declassification: Declassify hard disk drives only after approved
verification and review procedures are completed per Reference c.

3) Release: Unless otherwise specified by the appropriate IS Security
Officer (or equivalent), declassified hard disk drives may be released for disposal
or recycling only after sanitization procedures and a declassification review have
been completed per Reference c.

b. Diskettes

    1) Sanitization: Sanitize diskettes by using one of the following
procedures. Remove all labels or markings that indicate previous use or
classification.

        a) Degaussing: Degauss the diskettes in an NSA/CSS evaluated
degausser; see Reference b.

        b) Disintegration: Disintegrate diskettes using an NSA/CSS
evaluated disintegrator; see Reference d.

        c) Incineration: Material must be reduced to ash.

        d) Shredding: Shred diskettes using an NSA/CSS evaluated
crosscut shredder; see Reference e. Remove diskette cover and metal hub
prior to shredding.

    2) Declassification: Declassify diskettes only after approved verification
and review procedures are completed per Reference c.

    3) Release: Unless otherwise specified by the appropriate IS Security
Officer (or equivalent), declassified diskettes may be released for disposal or
recycling only after sanitization procedures and a declassification review have
been completed per Reference c.
OPTICAL STORAGE DEVICES

4. Optical storage devices include compact disks (CDs), digital versatile disks (DVDs), and Blu-ray disks (BDs).

   a. Sanitization: Sanitize optical storage devices using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

      1) Disintegration: Use an NSA/CSS evaluated disintegrator (see Reference d) to sanitize CD and DVD storage devices. BDs cannot be sanitized by this method.

      2) Embossing/Knurling: Use an NSA/CSS evaluated optical storage device embosser/knurler (see Reference f) to sanitize CD and DVD storage devices. BDs cannot be sanitized by this method.

      3) Grinding: Use an NSA/CSS evaluated optical storage device grinder (see Reference f) to sanitize CD storage devices. DVDs or BDs cannot be sanitized by this method.

      4) Incineration: Material must be reduced to ash.

      5) Shredding: Use an NSA/CSS evaluated optical storage device shredder (see Reference f) to sanitize CD and DVD storage devices. BDs cannot be sanitized by this method.

b. Declassification: Declassify optical storage devices only after approved verification and review procedures are completed per Reference c.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified optical storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed per Reference c.

SOLID STATE STORAGE DEVICES

5. Solid state storage devices include random access memory (RAM), read only memory (ROM), Field Programmable Gate Array (FPGA), Smart Cards, and flash memory.

   a. Sanitization: Sanitize solid state devices using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

      1) Disintegration: Disintegrate into particles that are nominally 2 millimeter edge length in size using an NSA/CSS evaluated solid state
disintegrator; see Reference g. It is highly recommended to disintegrate solid state storage devices in bulk lots with other storage devices.

2) Incineration: Material must be reduced to ash.

3) Power Removal: Sanitize DRAM (dynamic random-access memory), SRAM (static random-access memory), and Volatile FPGA by removing the power, including backup batteries. Once power is removed, sanitization is instantaneous.

4) Strip Shredding or Cutting: Sanitize Smart Cards using one of the following procedures.

   a) Strip Shredding: A strip shredder with a maximum width of 2 millimeters will destroy the microchip, barcode, magnetic strip and written information on the Smart Card. Smart Cards must be inserted diagonally into the strip shredder at a 45-degree angle for proper sanitization.

   \textit{NOTE: A CROSS CUT SHREDDER WILL NOT SANITIZE SMART CARDS.}

   b) Cutting: Cut the Smart Card into strips diagonally at a 45-degree angle, insuring that the microchip is cut through the center. Insure that the barcode, magnetic strip, and written information are cut into several pieces and the written information is unreadable.

b. Declassification: Declassify solid state storage devices only after approved verification and review procedures are completed per Reference c.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified solid state storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed per Reference c.

\textbf{HARD COPY STORAGE DEVICES}

6. Hard copy storage devices include paper, microforms, and cathode ray tube and plasma monitors with \textit{burn-in}.

   a. Sanitization: Sanitize hard copy storage devices using one of the following procedures.

   1) Sanitize paper by using one of the following procedures.

      a) Burning: Material must be reduced to ash.
b) Chopping, pulverizing, wet pulping: Material residue must be reduced to pieces 5 millimeters square or smaller.

c) Disintegration: Disintegrate paper using an NSA/CSS evaluated disintegrator; see Reference d.

d) Shredding: Shred paper using an NSA/CSS evaluated crosscut shredder; see Reference e.

2) Sanitize microforms by burning. Material must be reduced to ash.

3) Sanitize cathode ray tube and plasma monitors exhibiting burn-in by destroying the surface of the monitor into pieces no larger than 5 centimeters square.

b. Declassification: Declassify hard copy storage devices only after approved verification and review procedures are completed per Reference c.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified hard copy storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed per Reference c.

RESPONSIBILITIES

7. Information Assurance Standards Center for Storage Device Sanitization Research (Y2D123) shall provide technical guidance for the sanitization and release of IS storage devices.

8. NSA/CSS and all elements using this manual shall:

   a. Protect classified or sensitive information and make final decisions to declassify or release IS storage devices or refer to their IS security officer for guidance;

   b. Maintain records for the sanitization, declassification, and release of classified or sensitive information on IS storage devices when the procedures per this manual cannot be implemented due to time or fiscal constraints;

   c. Comply with Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation” (Reference h); and

   d. Ensure that all media considered to be Agency Owned Accountable Property (AOAP) is administered in accordance with NSA/CSS’s Property Management policies and procedures (Reference i). Proper documentation is needed for media that meets the AOAP criteria and is designated for destruction. This documentation will ensure the
accountability and traceability of all AOAP. For specific guidance on these policies and procedures please contact your organization’s Property Officer (“go property-officers”).

REFERENCES

9. References:


i. NSA/CSS Financial Management Manual 7-2, Volume 4, Chapter 6, “Property, Plant, and Equipment,” and Chapter 6 Annexes (various dates).

DEFINITIONS

10. Agency Owned Accountable Property(AOAP) – Includes (a) Capitalized PP&E (property, plant, and equipment) items (cost equals or exceeds the DoD capitalization threshold of $100,000); (b) PP&E items with a cost that is less than the DoD capitalization threshold but equals or exceeds the DoD accountability threshold of $5,000; (c) All personal and portable computing devices (e.g., desktop computers, laptops, PalmPilots (hand held computers), PDAs (personal digital assistant), and servers, including Special Government Design, regardless of cost); (d) Stewardship Land; (e) Heritage assets, regardless of cost; (f) Classified Items – material that requires protection in the interest of national security; (g) Sensitive Items – property requiring a high degree of protection and control as determined by legal and regulatory
requirements (for example: weapons, drugs); (h) Pilferable Items – property subject to theft for resale, personal use, or personal possession (for example: VCRs, televisions, or other items listed on the pilferable list (see FMM, Annex 7)). (Source: Annex 6 to Reference 1)

11. **Burn-In** – A tendency for an image that is shown on a display over a long period of time to become permanently fixed on the display. This is sometimes seen in emissive displays such as cathode ray tube and plasma, because chemical changes can occur in the phosphors when exposed repeatedly to the same electrical signals.

12. **Declassification** – An administrative decision/action, based on a consideration of risk by the owner, whereby the classification of a properly sanitized storage device is downgraded to UNCLASSIFIED.

13. **Degausser** – An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices or other magnetic material.

14. **Degaussing** (or Demagnetizing) – Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist.

15. **Information System (IS) Storage Devices** – The physical storage devices used by an IS upon which data is recorded.

16. **Recycling** – End state for IS storage devices processed in such a way as to make them ready for reuse, to adapt them to a new use, or to reclaim constituent materials of value.

17. **Sanitization** – The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, etc.