

ELECTRONIC MEDIA SANITIZATION

- 1. REASON FOR ISSUE:** This handbook establishes procedures for the sanitization of electronic storage media and information technology (IT) equipment that stores or processes VA information by, or on behalf, of the Department of Veterans Affairs (VA). This electronic storage media and IT equipment may require special disposition in order to mitigate the risk of unauthorized disclosure of veterans' benefits, health, or memorial information, and to ensure its confidentiality.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This handbook:
 - a. Establishes a consistent, standards-based policy for the sanitization of VA electronic media which stores or processes VA information by, or on behalf, of VA; and
 - b. Defines procedures to be implemented by VA staff to sanitize and document the sanitization of electronic media that store or process VA information by, or on behalf of, VA; and
 - c. Describes the responsibilities of the personnel involved in the sanitization process.
- 3. RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (OI&T) (005), DAS for Information Protection and Risk Management (005R), ADAS, Cyber Security (005R2).
- 4. RELATED DIRECTIVE:** VA Directive and Handbook 6500, *Information Security Program*.
- 5. RESCISSIONS:** None.

CERTIFIED BY:

/S/
Robert T. Howard
Assistant Secretary for Information and
Technology

**BY DIRECTION OF THE SECRETARY OF
VETERANS AFFAIRS**

/S/
Robert T. Howard
Assistant Secretary for Information and
Technology

Distribution: Electronic Only

ELECTRONIC MEDIA SANITIZATION**CONTENTS****PARAGRAPH**

1. PURPOSE.....	5
2. SCOPE/OVERVIEW	5
3. POLICY	6
4. RESPONSIBILITIES	9
a. Secretary of Veterans Affairs.....	9
b. Assistant Secretary for Information and Technology	9
c. Deputy Assistant Secretary for Information Protection Risk Management.....	9
d. Associate Deputy Assistant Secretary for Cyber Security	9
e. Deputy Assistant Secretary for Enterprise Operations and Infrastructure.....	9
f. Inspector General	10
g. General Counsel.....	10
h. Under Secretaries, Assistant Secretaries and Other Key Officials	10
i. Operating Unit Chief Information Officers (CIO).....	10
j. Facility Directors/Program Managers.....	10
k. Information Security Officers (ISO).....	10
l. Privacy Officers	11
m. Supervisors of Staff Officials Responsible for Performing the Sanitization Process	11
n. Staff Officials Responsible for Performing the Sanitization Process	11
o. Contracting Officers.....	12
p. Custodial Officer (Service Chief)	12
q. End Users	13
5. DECISION PROCESS	13
6. STANDARD MEDIA SANITIZATION PROCEDURES	16
a. Disposal.....	16
b. Clearing.....	16
c. Purging.....	17
d. Destroying.....	18
e. Contracting Sanitization Services for Electronic Media.....	19
f. Documentation.....	20
g. ISO Annual Review.....	21
7. REFERENCES.....	21

ELECTRONIC MEDIA SANITIZATION

APPENDICES

A: SANITIZATION CERTIFICATE	<u>A-1</u>
B: SANITIZATION REQUIREMENTS	<u>B-1</u>
C: ACRONYM LIST	<u>C-1</u>
D: DEFINITIONS	<u>D-1</u>

ELECTRONIC MEDIA SANITIZATION

1. PURPOSE: This Handbook sets forth policies and responsibilities for the proper sanitization of the Department of Veterans Affairs (VA) and non-VA Information Technology (IT) electronic media, which contain stored or processed sensitive and non-sensitive VA information prior to repair, disposal, reuse, or recycling.

2. SCOPE/OVERVIEW

a. Information disposition and sanitization decisions occur throughout the system life cycle. Critical factors affecting information disposition and media sanitization must be made at the start of a system's development. A determination must be made during the requirements phase concerning which media types will be used to create, capture, or transfer information used by the system. This analysis, balancing business needs and risk to confidentiality, will determine the media to be considered so that the system conforms to Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*.

b. Media sanitization and information disposition activities tend to be more intense during the disposal phase of the system life cycle. However, throughout the life of an information system, many types of media, containing sensitive and non-sensitive information, are transferred outside the direct control of VA. These transfers may be for maintenance reasons, system upgrades, or during a configuration update.

c. To ensure the confidentiality of the information being disposed, VA employees must sanitize all electronic storage media. This handbook identifies responsibilities, describes acceptable sanitization practices and procedures, and provides information on National Institute of Standards and Technology (NIST) and Federally-compliant, VA-accepted sanitization tools and equipment.

d. There are two primary types of media in common use:

(1) **Hard Copy:** Hard copy media are physical representations of information. Paper printouts, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into recycle bins and trash containers exposes VA to a significant vulnerability to "dumpster divers," and overly-curious employees. This creates a risk of accidental or unauthorized disclosure. Although the main focus of this Handbook is electronic media, sanitization procedures are also provided for some types of hard copy media. However, this Handbook is not intended to address the destruction of paper documents or paper printouts as VA Directive 6371, *Destruction of Temporary Paper Records*, covers this topic.

(2) **Electronic (or soft copy):** Electronic media are bits and bytes located on hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, and networking equipment. Other examples of electronic media used across VA facilities may include, but are not limited to copy machines, fax machines, printers, embossing machines, medical devices, and cameras.

e. This document details the sanitization of storage media prior to repair, reuse, disposal, or recycling, of that media by VA and non-VA entities.

f. This document applies to all electronic storage media and IT equipment which store or process sensitive and non-sensitive VA information by, or on behalf of, VA.

3. POLICY

a. VA sensitive information, sensitive information of other agencies (as defined to VA by the agencies) controlled or maintained by VA, or any other information not releasable to the public by VA, must be protected to prevent subsequent disclosure to unauthorized individuals, either within or outside VA. This includes electronic storage media and IT equipment containing VA sensitive information that is surplus, removed from VA control, or transferred to another VA component for reuse, which necessitates the removal of all information traces to prevent inadvertent information compromise.

b. Each VA office or facility, and all contractor facilities, must follow the security requirements and standards for the sanitization of electronic storage media contained in this handbook. Only software and/or procedures approved by the Office of Information and Technology (OI&T) will be used for sanitizing electronic storage media. VA employees must use the least destructive method for sanitizing electronic storage media, consistent with the standards in this Handbook, to foster re-utilization and minimize the generation of hazardous waste.

c. The VA Office of Inspector General (OIG) may issue a separate, more stringent electronic media sanitization policy, which OIG must follow, due to special security needs or resulting from the need to follow special procedures to ensure the admissibility of electronic evidence in legal proceedings.

d. VA offices and facilities notified by the Office of the General Counsel (OGC) that their IT equipment, electronic storage media, or information resident on either is subject to retention for possible litigation purposes, must immediately cease the repair, reuse, disposal, destruction, or sanitization of the involved equipment, storage media, or data. These restrictions also apply to non-VA IT equipment (including research equipment and/or grant-owned equipment), electronic storage media, and VA information resident on either.

e. Electronic storage media (hard disk drives, floppy diskettes, compact discs [CD]), containing VA sensitive information, are subject to the sanitization procedures provided in this Handbook, prior to their disposition or reuse by another person or entity. Employees, with the assistance of the local OI&T staff, will complete VA Form 0751, *Information Technology Equipment Sanitization Certificate*, contained in Appendix A of this document to validate and document the sanitization.

f. Also, VA Form 0751 must be completed and attached to the proper turn-in documentation, such as VA Form 2237, *Request, Turn-In, and Receipt for Property or Services*, as required by the local VA office or facility. It must then be submitted through the proper channels. The individual performing the sanitization, the supervisor of the individual performing the sanitization, and the Information Security Officer (ISO) must all sign VA Form 0751 after appropriate sanitization has been completed. The Custodial Officer is the official responsible for the Equipment Inventory Listing (EIL) and is responsible for maintaining the completed original form; the ISO is responsible for maintaining a copy of the completed form for audit/review purposes. This form will be maintained for a minimum of 3 years from the date of sanitization.

g. OI&T staff must train ISOs (and other designated staff assigned to perform media sanitization and/or process electronic storage media for sanitization) in VA data sanitization policies and procedures.

They must also provide current copies of any VA policies and documents describing or depicting sanitization methods and procedures to appropriate staff members.

h. Contracts involving media sanitization, electronic storage media, and IT equipment [sharing agreements, Memoranda of Understanding (MOU)], maintenance contracts, service contracts, and vendor repair agreements (including third party vendor repair, and lease agreements) must include the appropriate security language concerning the protection of VA assets including appropriate media sanitization for electronic storage media, and IT systems and equipment.

i. VA employees must protect VA sensitive information during maintenance and repair, or in other situations not requiring formal contracts or other written agreements with non-VA business associates (vendors, contractors, other government agencies). In these situations where the sanitization of VA IT equipment may not be feasible or appropriate, the VA employee must obtain a signed VA Form 0752, *Confidentiality of Sensitive Information Non-Disclosure Agreement*, from the non-VA business associate to whom the VA employee releases the equipment. The signed form must be given to and maintained by the ISO for a minimum of 3 years.

j. Users of non-VA leased or owned IT equipment including, but not limited to, personally-owned equipment (which requires an approved waiver from the VA Chief Information Officer [CIO]), vendor-owned, or research equipment obtained through a grant used to store, process, or access VA sensitive information are required to protect all VA sensitive information from subsequent disclosure to unauthorized persons during use and when the equipment is no longer used to access VA sensitive information.

k. VA employees must sanitize VA-leased IT equipment in accordance with this Handbook, the same as VA-owned equipment. Examples include electronic storage devices released for replacement or repairs, electronic storage devices returned to the vendor or manufacturer, and equipment that has reached the end of its lifecycle of use by VA.

l. All electronic storage media used in non-VA leased or owned IT equipment used to store, process, or access VA sensitive information are required to have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with this Handbook when the media are no longer used to access VA sensitive information, or when the media are disposed or removed from VA control.

m. At a minimum, the ISO must conduct and document an annual review of the sanitization process.

n. VA has a contracted, agency-wide program in place to sanitize and properly dispose of media containing VA sensitive information. ISOs are the points of contact (POC) for this program and facilitate all phases of the program for each Administration and staff office.

o. IT electronic media may be sanitized under a locally developed contract or in-house, whichever is deemed to be more cost-effective. Procedures for contracting sanitization services or completing services in-house are outlined in this Handbook and must be followed.

p. Returning leased equipment constitutes a risk; VA employees must sanitize VA sensitive information residing on leased equipment before releasing that equipment from direct VA control or ensure the contract states the media will not be returned upon termination of the contract. Depending upon the contract, this may include VA licensed software installed on leased equipment. Copyright-

protected software must be removed from equipment prior to repair, disposal, or reuse unless it will be reused by an agency component included as a part of the same group license under which the program was initially installed or is required to ensure the repair was successful. If installing Commercial Off the Shelf (COTS) Software, pre-approval is required by OI&T and the Contracting Officer. If the COTS software requires a user license limited to that individual, the individual must remove that software from the machine before releasing the machine for another individual's use.

q. Non-VA owned IT equipment including, but not limited to, personally-owned equipment (which requires an approved waiver from the VA CIO), vendor-owned, or research equipment obtained through a grant used to access VA sensitive information, constitutes a risk. When non-VA owned IT equipment is no longer used to access or store VA sensitive information, all equipment hard disk drives and internal memory is to be sanitized in accordance with Appendix B of this Handbook. All other electronic storage media used to store, process, or access VA sensitive information must be sanitized in accordance with Appendix B of this Handbook when the media are no longer used to access VA sensitive information being disposed of, or removed from VA control.

r. Electronic storage media must be safeguarded in the manner prescribed for the highest sensitivity of information processed on the computer equipment writing to that media, per the sensitivity categorization of the system documented in the system's security plan. Until the media are subject to approved clearing (overwriting), purging (degaussing), or destruction (disintegration, pulverization, melting, incineration, shredding, and sanding), it must be properly secured.

s. Maintenance of computer systems can introduce risks. Sanitization procedures will be considered by OI&T staff prior to non-VA personnel performing maintenance on computer equipment. If purging is impractical, prohibitively expensive, or could destroy the device, precautions must be taken to reduce the threat to VA sensitive information on the device. Non-VA maintenance personnel must be observed by VA personnel to ensure improper actions can be discerned and unauthorized disclosure prevented. VA employees will consult with the facility ISO, Contracting Officer, and, where appropriate, the facility Privacy Officer prior to granting access to contractors to VA IT systems to protect VA sensitive information from access, insertion, modification, or destruction. The facility will ensure the contract contains the appropriate privacy and security language for the protection of VA sensitive information. If a contractor is provided access to protected health information (PHI), as defined in Title 45, Code of Federal Regulations (CFR), Section 160.103, the facility, if within VHA, will also have to execute a Business Associate Agreement (BAA) or the facility, if in another component of VA, will execute VA Form 0752 with the contractor. VA IT equipment and electronic storage media removed from VA control are subject to the sanitization methods outlined in Appendix B of this Handbook, prior to their disposition or reuse by another individual or entity.

t. OI&T and facility property managers are required to report within VA usable excess IT equipment and redistribute that equipment for use, if appropriate. If the excess IT equipment cannot be used within the agency, then donations of equipment to schools (grades K-12) are encouraged under the auspices of Executive Order 12999 (Computers for Learning Program).

u. OI&T and facility property managers are encouraged to use VA's MOU established with UNICOR for processing scrap IT equipment and for the recycling of scrap electronic equipment, in general.

4. RESPONSIBILITIES: The responsibilities listed below are specifically related to media sanitization. For a listing of additional security responsibilities for these positions, see VA Directive and Handbook 6500.

a. **Secretary of Veterans Affairs** has designated the Assistant Secretary for Information and Technology as the Senior Agency Official responsible for ensuring sanitization procedures are performed on electronic storage media that store or retain VA information prior to repair, disposal, or reuse.

b. **Assistant Secretary for Information and Technology** is responsible for:

(1) Providing the resources (both funding and training) necessary to support the policy contained in this handbook; and

(2) Designating the Associate Deputy Assistant Secretary (ADAS) for Cyber Security as the principal official responsible for implementing this policy and establishing approved sanitization procedures.

c. **Deputy Assistant Secretary (DAS) for Information Protection Risk Management (IPRM)** Under the IT Single Authority, the VA CIO has created the DAS IPRM, which has authority over:

(1) VA enterprise cyber security budget; and

(2) Associate Deputy Assistant Secretary for Cyber Security.

d. **Associate Deputy Assistant Secretary (ADAS) for Cyber Security** is the VA Senior Agency Information Security Officer (SAISO) and is responsible for:

(1) Implementing the policies and procedures described in this handbook;

(2) Establishing agency-wide sanitization methods that are compliant with NIST standards and Federal requirements; and

(3) Providing standardized training on data media sanitization and disposal procedures to ISOs, IT staff, and other individuals designated to perform media sanitization and disposal.

e. **Director for IT Field Security Operations** is responsible for:

(1) Implementing and maintaining the VA national contract for media sanitization;

(2) Determining the VA approved sanitization technology and software products that are Federally and NIST compliant;

(3) Working in close association with Office of Cyber Security (OCS) to implement the policies and procedures contained in this handbook; and

(4) Providing resources necessary to implement the policies and procedures contained in this handbook.

f. **Deputy Assistant Secretary of Acquisition and Logistics** is responsible for proper disposal of all personal property which includes electronic media.

g. **Office of Inspector General (OIG)** will issue a separate electronic media sanitization policy (due to OIG requirements for evidence media handling and other special security needs) which only the OIG is required to follow.

h. **Office of the General Counsel (OGC)** is responsible for:

- (1) Interpreting laws, regulations, and directives applicable to electronic media sanitization; and
- (2) Rendering legal advice and services in the area of electronic media sanitization, upon request, to Under Secretaries, Assistant Secretaries, and Other Key Officials.

i. **Under Secretaries, Assistant Secretaries and Other Key Officials** are responsible for:

- (1) Working in close association with OCS to implement the policies contained in this handbook;
- (2) Providing resources necessary to implement the policies contained in this handbook; and
- (3) Ensuring the policies set forth in this Handbook are followed.

j. **Operating Unit CIOs** are responsible for providing necessary support to facility Directors/Program Managers and their staff in complying with this handbook.

k. **Facility Directors/Program Managers** are responsible for ensuring the policies set forth in this Handbook are followed by the individuals under his/her responsibility.

l. **ISOs** are responsible for:

- (1) Coordinating and overseeing VA's contracted Media Sanitization Program within his/her area of responsibility;
- (2) Reviewing VA Form 0751 with staff performing sanitization procedures, and certifying the process used to remove VA information complies with VA policy;
- (3) Maintaining copies of all completed sanitization certificates and associated documentation, as appropriate, for a minimum of 3 years for audit/review purposes;
- (4) Maintaining all signed original VA Forms 0752 for the facility/program office for a period of 3 years;
- (5) Reviewing the sanitization process annually, at a minimum, and documenting the results of the review, as outlined in this handbook; and

(6) Notifying the VA National Security Operations Center (NSOC) and/or the OIG of any suspected incidents within 1 hour of discovery, and assisting in the investigation of incidents, if necessary;

m. **Privacy Officers** are responsible for providing advice regarding the privacy issues surrounding the disposition of sensitive information and the media upon which it is recorded.

n. **Supervisors of Staff Officials Responsible for Performing the Sanitization Process**, are individuals including, but not limited to, IT CIOs, Biomedical Engineers, Research Directors, and other managers responsible for:

(1) Ensuring staff responsible for sanitization of electronic storage media is properly trained in the procedures for using approved methods in accordance with this policy;

(2) Ensuring and certifying, by signing VA Form 0751, only software and/or procedures approved by OI&T and VA policy are used to remove VA information from electronic storage media;

(3) Providing the completed, original VA Form 0751 to the official responsible for the Equipment Inventory Listing (EIL) and a copy of the form to the ISO;

(4) Ensuring coordination with the official responsible for the EIL and the ISO, prior to IT equipment leaving the VA facility for any reason, including repair or loan;

(5) Ensuring that all IT equipment leaving the facility for repair or loan has been annotated in the equipment record and has been issued a property pass;

(6) Obtaining a signed non-disclosure statement from non-VA business associates (vendors, contractors, other government agencies) and/or ensuring a BAA is on record for equipment removed from the facility for repair or other situations, where required; and

(7) Ensuring all signed original non-disclosure statements are provided to the ISO to maintain.

o. **Staff Officials Responsible for Performing the Sanitization Process** are individuals including, but are not limited to, the IT, biomedical, and research staffs, and other individuals designated by local management to sanitize media, are responsible for:

(1) Using the least destructive method for sanitizing IT equipment, consistent with the standards in this Handbook, to accomplish the required sanitization of data, to foster re-utilization, and to minimize the generation of hazardous waste;

(2) Ensuring and certifying, by signing VA Form 0751, only software and/or procedures approved by OI&T and VA policy are used to remove VA sensitive information from electronic storage media;

(3) Ensuring the sanitization certificate is provided to the supervisor of the staff performing the sanitization process for his/her certification;

(4) Coordinating the submission of IT equipment with the supervisor and ISO when sanitization is required for IT equipment, leaving the facility for any reason, including return of leased equipment, repair, loan; and

(5) Completing training in proper sanitization/disposal procedures.

p. Custodial Officer (Service Chief) – Official Responsible for the Equipment Inventory Listing (EIL) is responsible for:

(1) Ensuring all IT equipment submitted for disposition has completed VA Form 0751 and 2237 along with any additionally required local VA office or facility turn-in documentation;

(2) Coordinating with the staff official responsible for performing sanitization procedures (or other staff, as appropriate), prior to IT equipment leaving the facility for any reason, including return of leased equipment, repair, loan, or other reasons, when sanitization is required;

(3) Accepting IT equipment for disposal only when it is accompanied by properly completed turn-in documentation (VA Form 2237), completed VA Form 0751, and any local documentation requirements; and

(4) Maintaining a copy of all turn-in documentation, sanitization certificates, and other pertinent documents.

(5) Providing the original documentation to the Facility Accountable Officer for disposition processing and retention in accordance with VA Records Control Schedule.

q. Contracting Officers are responsible for:

(6) Ensuring security requirements are included in contracts involving IT equipment (sharing agreements, MOUs), maintenance contracts, vendor repair agreements (including third party vendor repair and/or lease agreements) to ensure sanitization of VA sensitive information is adequately performed in accordance with VA policy;

(7) Obtaining signed VA Form 0752, or ensuring a BAA is on record from non-VA business associates (vendors, contractors, other government agencies) when appropriate as defined by the policies set forth in this handbook; and

(8) Ensuring the ISO is provided signed copies of all non-disclosure statements for his/her audit/review records.

r. Facility Accountable Officers are responsible for:

(1) Assigning condition codes to equipment on VA Form 90-2237 which can be accomplished through coordination with the EIL Custodial Officer,

(2) Maintaining the original documentation (VA Form 0751 and 2237) and any other local documentation required in accordance with VA's Record Control Schedule.

s. **End Users** are individuals such as, but not limited to, affiliates, universities, business partners, researchers, non-VA and VA personnel, contractors, individuals that access VA systems remotely are responsible for:

(1) Complying with VA and local policies and procedures regarding the removal of VA information prior to repair, reuse, or disposal to include CIO approved personally-owned equipment used to access, store, or process VA sensitive information;

(2) Completing the VA annual information security awareness training program where the use, storage, and removal of VA sensitive information is addressed;

(3) Reporting suspected violations to his/her local ISO and facility Privacy Officer immediately upon detection in accordance with VA policy;

(4) Protecting VA sensitive information used in the performance of his/her duties; and

(5) Minimizing unnecessary use of VA sensitive information.

5. DECISION PROCESS

The decision as to which type of sanitization method to use is commensurate with the security categorization of the information, not the media type. This determination is made during the early stages of the development or procurement of the system based on FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. When media contain information categorized at different levels, the media must be sanitized according to the highest level of data/information categorized on the media. The system's information categorization is documented in the system's security plan (SSP). The following summary is a textual equivalent of the flowchart on the following page:

a. If the security categorization of the information is LOW and the information is:

(1) Not leaving organizational control, clear the information, validate (certify) and document the clearance. (See Section 6 of this Handbook, Standard Media Sanitization Procedures, for details on the clearing process.)

(2) Leaving organizational control, purge the information, validate (certify) and document the purge. (See Section 6 of this Handbook for details on the purging process.)

b. If the security categorization of the information is MODERATE and the media are:

(1) To be reused within VA, then clear the media, validate (certify) and document the clearance.

(2) To leave VA's control, purge the media, validate (certify) and document the purge.

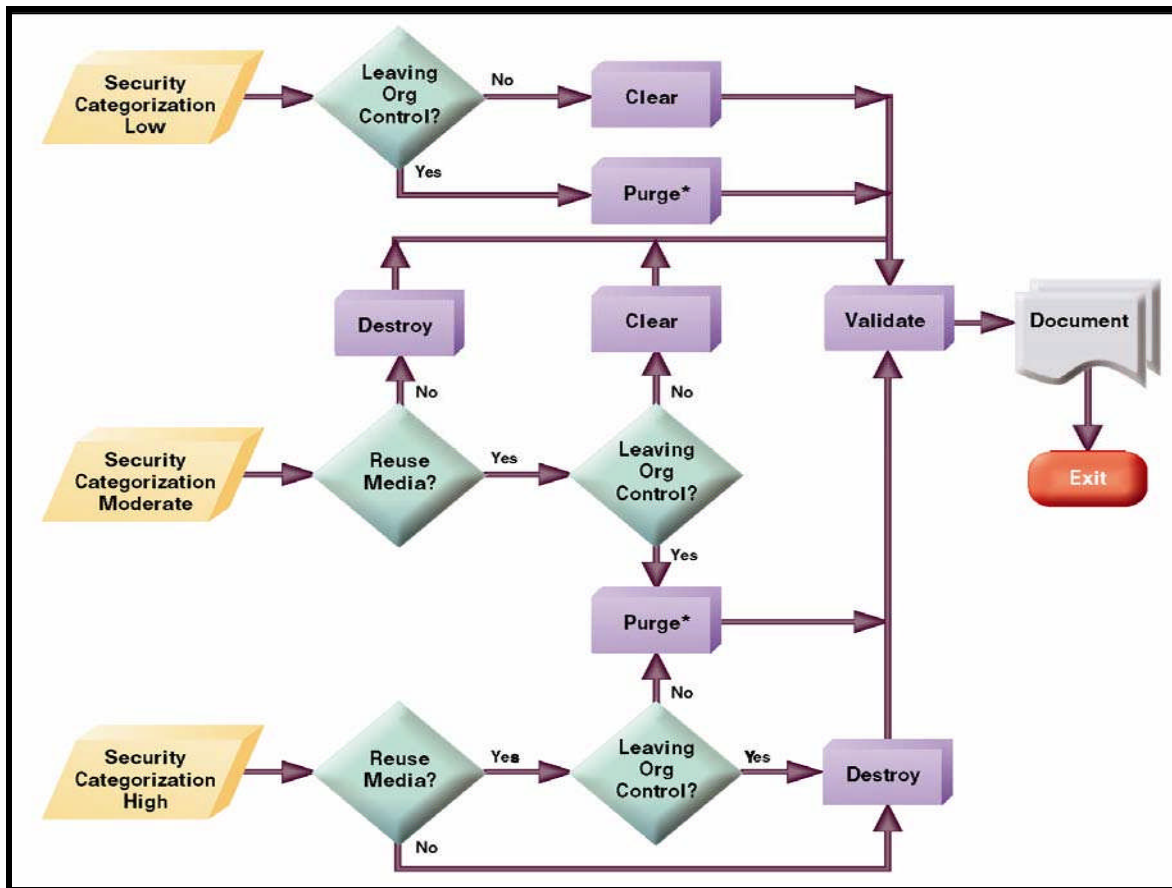
(3) Not to be reused, destroy the media, validate (certify) and document the destruction.

c. If the security categorization of the information is HIGH and the media are to:

(1) Be reused and is not leaving the control of VA, purge the media, validate (certify) and document the purge.

(2) Leave the control of VA, destroy the media, validate (certify) and document the destruction.

d. The following flow chart, provided by NIST, is to be used in making sanitization decisions commensurate with the security categorization of the confidentiality of the information, not the type of media. The chart reflects the process described in paragraph 5.a – 5.c.



* For some media, clearing media does not suffice for purging. However, for Advanced Technology Attachment (ATA) hard disk drives manufactured after 2001 (over 15GB), the terms clearing and purging have converged.

6. STANDARD MEDIA SANITIZATION PROCEDURES

a. **Disposal** is the act of discarding media with no other sanitization considerations. This is frequently used for recycling paper that does not contain VA sensitive information, but may also include other media. All waste paper or discarded materials, from any department containing sensitive personal information (SPI) must be either shredded or placed in locally approved locked containers for later collection and shredding. Shredding must be accomplished in accordance with the procedures outlined in VA Directive 6371.

b. Clearing

(1) Clearing information is a level of media sanitization protecting the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities; it must be resistant to keystroke recovery attempts, executed from standard input devices and from data scavenging tools.

(2) Overwriting is an acceptable method for clearing media, but only if the media are to be reused within VA. Overwriting is a clearing process in which random data are written over storage locations previously held by sensitive information. Overwriting cannot be used for media that have been damaged or that are not rewriteable, according to NIST SP 800-88, *Guidelines for Media Sanitization*, and the media type and size may also influence whether overwriting is a suitable sanitization method. See Appendix B of this Handbook for media and the associated, acceptable clearing methods.

(3) To clear magnetic media, all memory locations are overwritten a minimum of three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character). The success of the overwrite procedure is verified through random sampling of the overwritten media.

(4) Magnetic media that have been cleared must remain at the previously designated security category (for confidentiality) and secured in a controlled environment. Only software and/or procedures approved by OCS shall be used for clearing magnetic media. Magnetic media that have been cleared by overwriting may only be reused within the VA boundaries and within the previously assigned security category.

(5) Overwriting is not 100 percent successful when media contain unusable sectors, blocks, or "bad" tracks in a magnetic disk, drive, or inter-record gaps in magnetic tapes. Original data, written to the damaged sector prior to it becoming defective, will not be overwritten and any information previously recorded in these areas can be recovered with specialized tools and techniques. Before magnetic media are used, all usable tracks, sectors, or blocks should be identified. For all media found with damaged sectors, overwriting is not an acceptable clearing method.

(6) Operating system-level deletion and, especially, overwriting do not ensure the complete sanitization of media; therefore, these methods are only used to sanitize media containing non-VA sensitive information. Overwriting cannot be used for media that have been damaged or that are not rewriteable, according to NIST SP 800-88. A compromise of sensitive data may occur if media are released when an addressable segment of a storage device (such as, unusable, or "bad" tracks in a disk drive, or inter-record gaps in tapes) is not receptive to an overwrite. As an example, a disk may develop

unusable tracks or sectors during ordinary operation; however, sensitive data may have been previously recorded in these areas. It may be difficult to overwrite these unusable tracks. If this occurs and these tracks cannot be overwritten, sensitive information may remain on these tracks. In this case, overwriting is not an acceptable method and the media must be degaussed or destroyed.

- (7) The size of the media may influence whether overwriting is a suitable sanitization method.

c. Purging

- (1) Purging is the sanitization, or removal, of data from a system or storage device with the intent of the data not able to be reconstructed by laboratory techniques. For some media, clearing does not suffice for purging. However, for ATA hard disk drives manufactured after 2001 (over 15GB), the terms clearing and purging have converged. A laboratory attack involves a threat using advanced equipment, resources, and knowledge to conduct data recovery attempts on media outside its normal operating environment.

- (2) Executing the Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. The sensitivity of the data stored on the computer and the feasibility of software purging should be weighed before degaussing hard drives. Degaussing of any hard drive assembly usually destroys the drive, as the firmware that manages the device is also destroyed. NIST SP 800-88, *Guidelines for Media Sanitization*, includes a reference to the software, Secure Erase, from the University of California, San Diego (UCSD) Center for Magnetic Recording Research (CMRR) site and a link for downloading.

- (3) Degaussing is exposing magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (low energy or high energy) of magnetic media they can purge and operate using either a strong permanent magnet or an electromagnetic coil. Degaussing is an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. In some circumstances, degaussing does not guarantee complete data destruction. For example, using under-strength degaussing equipment will not ensure complete data purging. Always ensure the appropriate degaussing equipment is matched with the media being degaussed. Proper degaussing will ensure insufficient magnetization left behind in a medium (referred to as data remanence) to reconstruct the data. Degaussing is not effective for purging non-magnetic media, such as optical media CDs or digital versatile discs (DVD) and these must be destroyed.

- (4) VA approved degaussers are those which have been tested and approved by the National Security Agency (NSA). NSA publishes a list of evaluated degaussers, the Degausser Products List (DPL). A current copy of the DPL is available at www.nsa.gov. The introduction to the DPL explains how to determine the appropriate degausser for magnetic tape and magnetic disk media. Do not assume all of the degaussers listed are capable of erasing all formats of magnetic tape or magnetic disk media.

- (5) Degaussing has risks which must be mitigated; incorrect usage of degaussing equipment can compromise data residing on storage media. For example, storage media removed before the degaussing cycle is complete will create data remanence on the storage media. Another risk involves using the wrong degausser for a specific media.

Correctly labeling the coercivity of the media will help mitigate this risk. Use the NSA DPL for definitions and coercivity levels of magnetic tapes, magnetic disks, and approved degaussers.

(6) Degaussing equipment must be tested and certified periodically. Preventive maintenance must occur on a regular schedule to preclude mechanical or electrical problems. Some manufacturers have maintenance contracts and recommended maintenance schedules to ensure the integrity of the degaussing procedure. After installation, a degausser must be tested every 6 months for its first 2 years of operation and annually thereafter, as specified in the current NSA DPL. Verify with the manufacturer of the equipment if specific testing procedures are used. Test and diagnostic equipment used on devices with storage media can collect sensitive information; therefore, test and diagnostic devices must be purged after use to safeguard against this risk.

(7) Magnetic media stored for an extended period of time or under high temperature (exceeding 120 degrees Fahrenheit) becomes difficult to degauss. Each facility should have a media rotation process and is responsible for providing a stable environment for magnetic media storage. If purging media is not a reasonable sanitization method, magnetic media containing VA sensitive information must be destroyed.

(8) Ensuring labels are applied to magnetic tapes to identify the coercivity of the media upon initial use: Magnetic disk coercivities are identified by date of manufacture or date of purchase. Maintain a list of magnetic disk drive models, serial numbers, and purchase dates upon initial use. Strict inventory controls should be in place to ensure magnetic tape and disk coercivities can be identified so the correct purge procedure is used for sanitization of the magnetic media.

d. Destroying

(1) Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods including disintegration, incineration, pulverizing, shredding, and melting.

(2) If destruction is decided upon, due to the high security categorization of the information or due to environmental factors, any residual medium must be able to withstand a laboratory attack. The following are destruction methods:

(a) Disintegration, Incineration, Pulverization, and Melting: These sanitization methods are designed to completely destroy media. These methods are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

(b) Shredding: Paper shredders may be used to destroy flexible media, such as diskettes, once the media are physically removed from their outer containers. The shred size of the refuse must be small enough so there is reasonable assurance, in proportion to the data confidentiality level, that the information cannot be reconstructed. Refer to VA Directive 6371 for shredding requirements.

(3) Optical mass storage media, including compact disks (CD, CD_R, CD-RW, and CD-ROM), DVDs, and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning.

When material is disintegrated or shredded, all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²).

(4) Prior to destroying electronic media that do not contain VA sensitive information and is to be reused within VA, an attempt to sanitize the media by using an approved clearing procedure must be performed in order to minimize the potential generation of hazardous waste and to foster reuse. The following electronic media that have reached the end of its life cycle for use within VA must be sanitized by degaussing and destruction: magnetic tape, reels, cassettes, cartridges, magnetic disks, and optical disks. Destruction of electronic media will be performed in accordance with the National Security Agency (NSA)/Central Security Service (CSS) *Storage Device Declassification Manual*, and *NSA Evaluated Destruction Devices*, available at www.nsa.gov. Destruction of media can only be conducted by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction. The handling of hazardous materials, if any, must be in compliance with applicable environmental laws and regulations. The following methods will be used to destroy media:

- (a) Destruction by smelting (to melt or fuse) at an approved metal destruction facility; or
- (b) Destruction by pulverization or disintegration (crushing or grinding, reducing media to very small particles, as defined by NSA guidance), at an approved metal destruction facility; and
- (c) The use of an NSA approved destruction device to ensure media are physically destroyed.

e. Contracting Sanitization Services for Electronic Media

(1) In some cases, such as refreshing a large number of leased computers, it may prove more cost-effective to obtain sanitization services for IT equipment and/or electronic storage media through a contract as opposed to VA personnel performing the sanitization.

(2) VA OI&T has a contracted program in place to sanitize and properly dispose of electronic media containing VA sensitive data and information. The contract allows for “degaussing and destruction” or “degaussing and returning.” ISOs are the points of contact (POC) for this program and facilitate all phases of the program for each Administration and staff office. The *Media Sanitization and Destruction User Guide* is available on the VA Information Protection Portal.

(3) If an Operating Unit elects to use a different contracting vehicle other than the one provided by OI&T, the following procedures are required:

- (a) The language contained in VA Form 0752 must be included in all contracts, pertaining to sanitization services.
- (b) At a minimum, the contract must specify the contractor will employ the sanitization methodologies and procedures outlined in this handbook- this includes completion of VA Form 0751. The certificate must be completed by the contractor and provided to the Facility Accountable Officer/Contracting Officer. The ISO will be provided a copy for their records.
- (c) IT equipment and/or electronic storage media must be securely delivered to the contractor (using FedEx White Glove Service, USPS Registered Mail, and/or other classified carriers with

signature service). Alternatively, the contractor may pick up the devices from the VA facility or program office, in accordance with local procedures.

(d) Transfer of the IT equipment and/or electronic storage media between the contractor and the VA facility or program office must be coordinated with the Accountable Officer/Property Manager, the official responsible for the EIL, and the ISO, to ensure adequate tracking of the devices at all times.

(e) Contract personnel engaged in media sanitization contracts for VA will have background investigations performed according to the specifications outlined in VA Directive 0710, *Personnel Suitability and Security Program*.

f. Documentation

(1) For all IT equipment required to be turned-in through the local Custodial Officer, VA Form 0751 must be completed and attached to any additional local turn-in documentation and submitted through the proper channels, as outlined by local facility procedures.

(2) Other IT equipment and electronic storage media (magnetic disk drives or any device not tracked on the EIL) containing VA sensitive information is subject to sanitization procedures prior to disposition, reuse, or release outside of VA boundaries, or otherwise removed from VA control. VA Form 0751 must be completed and provided to the Custodial Officer and a copy maintained by the ISO for audits/reviews.

(3) IT equipment or electronic storage media requiring sanitization will have the following information documented and maintained at the local facility for a minimum of 3 years from the date of disposition. Appendix A must be used as the documentation tool that provides the following information:

- (a) A description of the media (make, model, brand, type);
- (b) Equipment inventory tracking number ("EE" number, if applicable);
- (c) Equipment serial number, if applicable;
- (d) Date of sanitization;
- (e) A description of the sanitization method used;

(f) If clearing (for non VA sensitive information and reuse within VA only), include the certificate generated by the clearing software; and

(g) The recommended condition code of the equipment. (Condition codes: 4-Usable, 7-Repairable (if repairable, describe repairs needed), X-Salvage, or S-Scrap)and;

(h) The names and signatures of the personnel executing the procedures, the individual's supervisor, and the ISO validating the sanitization methods used.

g. ISO Annual Review.

(1) ISOs are responsible for reviewing the sanitization process at their facility or program office on an annual basis, at a minimum, and for remediating any issues identified during the review.

(2) The ISO's annual review must demonstrate adequate sanitization documentation is maintained (media requiring sanitization are appropriately recorded using VA Form 0751) and procedures established in this Handbook are appropriately followed. Discussions with IT staff, OA&MM, and/or other staff involved in the sanitization process are recommended to ensure those individuals are aware of, and adhere to, the requirements established in this handbook and the associated directive.

(3) Results of the review and remediation must be documented in writing and maintained by the ISO for 3 years.

7. REFERENCES

- a. E-Government Act of 2002, Public Law 107-347 § 208, 116 Stat.2899, 2921 (2002)
- b. Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- c. Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- d. Federal Management Regulation (FMR) 102-36, *Disposition of Excess Personal Property*
- e. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 § 264, 110 Stat. 1936, 2003
- f. National Archives and Records Administration General Records Schedule
- g. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 1, *Recommended Security Controls for Federal Information Systems*
- h. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*
- i. National Security Agency (NSA)/Central Security Service (CSS) *Storage Device Declassification Manual*
- j. Privacy Act of 1974, 5 U.S.C. 552a
- k. Resource Conservation and Recovery Act of 1976
- l. VA Directive 6371, *Destruction of Temporary Paper Records*
- m. VA Directive 6600, *Responsibility of Employees and Others Supporting VA in Protecting Personally Identifiable Information (PII)*

- n. VA Directive 7125, *Acquisition and Material Management Policy—General Procedures*
- o. VA Directive 7127, *Material Management Procedures*
- p. VA Directive and Handbook 0710, *Personnel Suitability and Security Program*
- q. VA Directive and Handbook 6500, *Information Security Program*.

APPENDIX A: SANITIZATION CERTIFICATE

This is the form required to validate and document the Sanitization Process.

Department of Veterans Affairs		INFORMATION TECHNOLOGY EQUIPMENT SANITIZATION CERTIFICATE										
NAME OF FACILITY/ORGANIZATION VA VAMC/PO/RO				FACILITY/ORGANIZATION NUMBER 123456789		DATE 07/26/2009						
EQUIPMENT DESCRIPTION <i>(Make, Model, Brand, Type)</i>	INVENTORY TRACKING NO. <i>(e.g., "EE" number)</i>	SERIAL NUMBER	DATE SANITIZED	METHOD USED TO REMOVE DATA <i>(OCS Authorized Only)*</i>	CONDITION CODE **	COMMENTS FOR CONDITION CODE 7 <i>(Repairable)(Describe repairs needed)</i>						
Seagate Hard Drive	123456789	98765 4321 78945 1	07/25/2008	Data Eraser	7	Reuse of hard drive within VAMC						
West Hard Drive	9564123575	125 6988 12312 111 2	04/04/2008	Data Eraser	X							
<p>* Attach certificates of sanitization generated by disk wiping tool (if available), in addition to VA Form 2237, Request for Turn in and Receipt for Property or Services.</p> <p>** Condition Codes: Usable (4), Repairable (7), Salvage (X), or Scrap (S).</p> <p>CERTIFICATION: I certify that I have evaluated this Information Technology (IT) device(s) and have performed steps to remove all sensitive data through a process that has been deemed to be in compliance with VA policy.</p> <table><tr><td>PRINTED NAME</td><td>SIGNATURE</td><td>TITLE, STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS</td><td>DATE</td></tr></table>							PRINTED NAME	SIGNATURE	TITLE, STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS	DATE		
PRINTED NAME	SIGNATURE	TITLE, STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS	DATE									
<p>CERTIFICATION: I certify that the staff official performing the sanitization process (above), used approved sanitization methods to remove sensitive information from this device(s).</p> <table><tr><td>PRINTED NAME</td><td>SIGNATURE</td><td>TITLE, SUPERVISOR OF STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS</td><td>DATE</td></tr></table>							PRINTED NAME	SIGNATURE	TITLE, SUPERVISOR OF STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS	DATE		
PRINTED NAME	SIGNATURE	TITLE, SUPERVISOR OF STAFF OFFICIAL RESPONSIBLE FOR PERFORMING SANITIZATION PROCESS	DATE									
<p>CERTIFICATION: I certify that I have reviewed with the staff official performing the sanitization process (above), the process used to remove sensitive information from this device(s), and concur that the process used complies with VA policy.</p> <table><tr><td>PRINTED NAME</td><td colspan="3">SIGNATURE OF INFORMATION SECURITY OFFICER</td><td colspan="2">DATE</td></tr></table>							PRINTED NAME	SIGNATURE OF INFORMATION SECURITY OFFICER			DATE	
PRINTED NAME	SIGNATURE OF INFORMATION SECURITY OFFICER			DATE								

[illegible]

APPENDIX B: SANITIZATION REQUIREMENTS

Media Type	Clear	Purge	Physical Destruction
Hard Copy Storages			
Archived X-ray film	See Physical Destruction	See Physical Destruction	Once archived in accordance with Records Control Schedule 10-1, film must be kept secure to avoid compromise of patient data until it can be sent in accordance with IL 0490-07-07 dated April 17, 2007, to the VA Service and Distribution Center (SDC), Hines, IL. Film is consolidated by the SDC and shipped to a recycler where it is destroyed during silver recovery processing.
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 hard reset to reset the PDA to factory state. Contact the manufacturer for proper sanitization procedure.	Same as Clear.	Incinerate PDAs by burning the PDAs in a licensed incinerator. Shred. Pulverize.
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.
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.

Appendix B

Media Type	Clear	Purge	Physical Destruction
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 agency-approved software and validate the overwritten data.	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 agency-approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> 1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. 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. 3. Purge media by using agency-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 agency-approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> 1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
		<p>2. 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.</p> <p>3. Purge media by using agency-approved and validated purge technologies/tools.</p>	
Zip Disks	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Degauss using a NSA/CSS-approved degausser. Degaussing any current generation zip disks will render the disk permanently unusable.	Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. Shred.
SCSI Drives	Overwrite media by using agency-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. Degaussing any current generation hard disk will render the drive permanently unusable.	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	<p>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.</p> <p>Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified 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.</p>	<p>Degauss using an NSA/CSS-approved degausser.</p> <p>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.</p>	<p>Incinerate by burning the tapes in a licensed incinerator.</p> <p>Shred.</p> <p>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.</p>

Media Type	Clear	Purge	Physical Destruction
Optical Disks			
CDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <ol style="list-style-type: none"> 1. Removing the Information bearing layers of CD media using a commercial optical disk grinding device. 2. Incinerate optical disk media (reduce to ash) using a licensed facility. 3. 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 mm²). This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm².
DVDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations.</p> <ol style="list-style-type: none"> 1. Removing the Information bearing layers of DVD media using a commercial optical disk grinding device. 2. Incinerate optical disk media (reduce to ash) using a licensed facility. 3. 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 mm²). This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.
Memory			
Compact Flash Drives, SD	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	See Physical Destruction.	<p>Destroy media in order of recommendations:</p> <ol style="list-style-type: none"> 1. Shred. 2. Disintegrate. 3. Pulverize. 4. Incinerate by burning in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
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 data sheets.	Same as Clear.	Shred. Disintegrate. Pulverize.
Electronically Erasable PROM (EEPROM)	Overwrite media by using agency approved and validated overwriting technologies/methods/tools. Remove all labels or markings that indicate previous use or confidentiality.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.

APPENDIX C: ABBREVIATIONS/ACRONYMS USED IN HANDBOOK AND APPENDICES

Abbreviation / Acronym	Description
ADAS	Associate Deputy Assistant Secretary
ATA	Advanced Technology Attachment
BAA	Business Associate Agreement
CD	Compact Disc
CD-ROM	Compact Disc Read Only Memory
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COTS	Commercial off the Shelf
CMRR	Center for Magnetic Recording Research
CSS	Central Security Service
DAS	Deputy Assistant Secretary
DPL	Degausser Products List
DVD	Digital Versatile Disc
EIL	Equipment Inventory Listing
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMR	Federal Management Regulation
HIPAA	Health Insurance Portability and Accountability Act
IPRM	Information Protection and Risk Management
ISO	Information Security Officer
IT	Information Technology
MO	Magneto-Optic
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSOC	Network Security Observation Center
OA&MM	Office of Acquisition and Material Management
OCS	Office of Cyber Security
OGC	Office of General Council
OIG	Office of the Inspector General
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
PHI	Protected Health Information
PII	Personally Identifiable Information
POC	Point of Contact
RAM	Random Access Memory
ROM	Read-Only Memory
SAISO	Senior Agency Information Security Officer
SP	Special Publications
SPI	Sensitive Personal Information
SSP	System Security Plan

Abbreviation / Acronym	Description
UCSD	University of California, San Diego
USC	United States Code
VA	Department of Veterans Affairs

APPENDIX D: DEFINITIONS

Glossary Term	Definition
Business Associate Agreement	A covered entity's contract or other written arrangement with its business associate. The agreement must contain the elements specified at 45 CFR 164.504(e). For example, the contract must: (1) Describe the permitted and required uses of protected health information by the business associate; (2) Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and (3) Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.
CD	Compact Disc: a class of media on which data are recorded by optical means.
CD-R	Compact Disc Recordable: A CD that can be written on only once but read many times. Also known as WORM.
CD-RW	Compact Disc Read/Write: A CD that can be purged and rewritten multiple times.
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations.
CMRR	The Center for Magnetic Recording Research (CMRR) advances the state-of-the-art in magnetic storage, and trains graduate students and postdoctoral professionals. The Center is located at the University of California, San Diego.
Coercivity	Measured in oersteds (Oe), it is a property of magnetic material used as a measure of the amount of applied magnetic field (of opposite polarity) required to reduce magnetic induction to zero from its remnant state (i.e., taking the media from a recorded state to an unrecorded state). Values on specific equipment should be available from the manufacturer or vendor.
Data	Pieces of information from which "understandable information" is derived.
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI, and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors.
Destruction	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.
Digital	The binary coding scheme generally used in computer technology to represent data as binary bits (1s and 0s).
Disintegration	A physically destructive method of sanitizing media; the act of separating into component parts.
Disposal	The act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
Disposal of IT Equipment	Equipment that is destroyed, excessed, transferred, surplused, discontinued from rental or lease, exchanged, donated, sold, or otherwise released from VA control.
DVD	Digital Video Disc – a disc the same shape and size as a CD; but the DVD has a higher density and gives the option for data to be double-sided or double-layered.

DVD-RAM	A disk that can be recorded and erased repeatedly but are only compatible with devices manufactured by the companies that support the DVD-RAM format. DVD-RAM discs are typically housed in cartridges.
DVD-RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD Forum.
DVD+RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD+RW Alliance.
DVD+R	A write-once (read only) version of the DVD+RW optical disk from the DVD+RW Alliance.
DVD-R	A write-once (read only) DVD disk for both movies and data endorsed by the DVD Forum.
Electronic Media	General term that refers to media on which data are recorded via an electrically based process. This includes electronic storage media such as floppy disks, CDs, hard disk drives, memory sticks, and audio or videotapes that contain VA sensitive information.
Erasure	Process intended to render magnetically stored information irretrievable by normal means.
FIPS	Federal Information Processing Standards.
Format	Pre-established layout for data.
Hard Disk	A rigid magnetic disk fixed permanently within a drive unit and used for storing data.
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes.
Information	Meaningful interpretation or expression of data.
Information Technology (IT) Equipment	For purposes of this handbook, IT equipment requiring sanitization is identified as any electronic IT device that contains VA sensitive information (e.g., Blackberry pagers; personal digital assistants (PDA); facsimile machines; desktop computers; laptops; printers with memory capability; and business, IT, or medical equipment/devices with magnetic disk drives; other memory retaining devices that contain VA sensitive information).
Keyboard Attack	In a keyboard attack, information is scavenged through system software capabilities (e.g., advanced software diagnostic tools).
Laboratory Attack	In a laboratory attack, information is scavenged through the use of more sophisticated equipment or other elaborate means.
Media	Plural of medium.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
Melting	A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat.
Memo of Understanding	The Memorandum Of Understanding/Memorandum Of Agreement (MOU/MOA) documents the terms and conditions for sharing data and information resources. It defines the purpose of the interconnection, identifies relevant authorities, specifies the responsibilities of each organization, defines the apportionment of costs, and identifies the timeline for terminating or reauthorizing the interconnection.
Oersted	A unit of magnetic field strength.

Optical Disks	A plastic disk that is “written” (encoded) and “read” using an optical laser device. The disc contains a highly reflective metal and uses bits to represent data by containing areas that reduce the effect of reflection when illuminated with a narrow-beam source, such as a laser diode.
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. See comments on clear/purge convergence.
Pulverization	A physically destructive method of sanitizing media; the act of grinding to a powder or dust.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods. See comments on clear/purge convergence. Purging is a more aggressive form of sanitization than clearing.
Read	Fundamental process in an information system that results only in the flow of information from an object to a subject.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disc.
Recovery Procedures (recoverable)	Action necessary to store data files of an information system and computational capability after a system failure.
Remanence	Residual information remaining on storage media after clearing. This residual information may allow data to be reconstructed using special forensic techniques and recovery tools. (The goal of this handbook is to provide procedures that will reduce data remanence to acceptable levels.)
Residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.
Reuse	For purposes of this handbook, reuse is defined as the process of placing electronic storage media or IT equipment back into service after it has already been in service (e.g., a device used by one individual or entity passed along to a different individual or entity).
ROM	Read Only Memory. Generally a commercially available disc or solid state device on which the content was recorded during the manufacturing process.
Sanitize	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Secure Erase	An overwrite technology using firmware based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure. It was added to the ATA specification in part at CMRR request. For ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command and successfully pass secure erase validation testing at CMRR. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives tested by CMRR. SCSI drives are a small percentage of the world’s hard disk drives, and the command will be implemented when users demand it.
Sensitive Personal Information (SPI)	The term, with respect to an individual, means any information about the individual maintained by an agency, including the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) Information that can be used to distinguish or trace the individual’s identity, including name, social security number, date and place of birth, mother’s maiden name, or biometric records.
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
Smelt	To melt or fuse metal.

Storage Media	Any device or hard copy method for the retention of applications and data so that they are available for use. Storage media include: paper, hard drives, removable drives (such as Zip disks), CD-ROM or CD-R discs, DVDs, flash memory, USB drives, and floppy drives.
Unauthorized Access	Gaining logical or physical access to VA information or information systems either without authorization or in excess of previously authorized access.
VA Sensitive Information	All Department data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.
WORM	Write Once Read Many. Refers to a data storage technology that allows information to be written to a disk a single time and prevents the drive from erasing the data. The disks are intentionally not rewritable, because they are especially intended to store data that the user does not want to erase accidentally.
Write	Fundamental operations of an information system that results only in the flow of information from a subject to an object.