



## **Media Disposition and Sanitation Procedure**

## Revision History

Version	Date	Editor	Nature of Change
1.0	11/14/06	Kelly Matt	Initial Release

## Table of Contents

1.0 Overview.....	1
2.0 Purpose.....	1
3.0 Scope.....	1
4.0 NIST Guidelines .....	1
5.0 Information Protection and Media Disposition.....	1
5.1 Primary Media Types.....	1
Hard Copy:.....	1
Electronic (or soft copy): .....	1
6.0 Sanitization .....	2
6.1 Sanitization Methods .....	2
6.2 Sanitization Guidelines .....	3
7.0 Enforcement.....	8
8.0 Related Policies, Procedures, and Codes of Conduct. ....	8

## **1.0 Overview**

Media disposition is a key element in assuring data confidentiality. Confidentiality is the ability to restrict access to information based on the value of the information. This includes protecting personally identifiable information.

In order to provide appropriate controls on the information we are responsible for safeguarding, we must properly dispose of media in all forms.

## **2.0 Purpose**

This document aids in establishing clear guidelines for media disposition and sanitation.

## **3.0 Scope**

This Procedure applies to employees, contractors, consultants, temporary employees, and other workers at UNC including all personnel affiliated with third parties.

## **4.0 NIST Guidelines**

This procedure has been adapted for the University of Northern Colorado from the National Institute of Standards and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization. The information and recommendations made in this document have drawn heavily on the guidelines set forth by the NIST special publication.

This adaptation has been developed for internal use. The express intent of this document is to provide a simplified and tailored approach to manage and implement the NIST guideline within UNC.

## **5.0 Information Protection and Media Disposition**

In order for UNC to have appropriate controls on the information it is responsible for safeguarding, it must properly safeguard the media used. An often rich source of illicit information collection is through dumpster diving for improperly disposed hard copy media or through reconstruction of data on media not sanitized in an appropriate manner. Media flows in and out of an organizations control through recycle bins in paper form, out to vendors for equipment repairs, and hot swapped into other systems in response to emergencies. This potential vulnerability can be mitigated through proper understanding of where information is located, what that information is and how to protect it.

### ***5.1 Primary Media Types***

#### **Hard Copy:**

Hard copy media is physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platen are all examples of hard copy media. These types of media are often the most uncontrolled. Information tossed into the recycle bins and trash containers exposes a significant vulnerability to “dumpster divers”, and overcurious employees, risking accidental disclosures.

#### **Electronic (or soft copy):**

Electronic media are the bits and bytes contained in hard drives, USB removable media, disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in section 6.2.

Media will continue to advance and evolve over time. The processes described in this document should guide media sanitization decision making regardless of the type of media in use.

## 6.0 Sanitization

Several different methods can be used to sanitize media. Four of the most common are presented in this section. Individuals should assess the media to be disposed of and determine the future plans for the media. Then, using information in the tables below, decide on the appropriate method for sanitization.

To facilitate secure disposition of electronic media UNC Information Technology provides a secure drop service in the basement of Carter Hall at the operator's window. Individuals can bring digital media to this area and for secure disposal.

### 6.1 Sanitization Methods

#### Sanitization Methods

Method	Description
Disposal	Disposal is 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.
Clear	One method to sanitize media is 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. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method. Two approved software tools are Secure Erase which can be download from the University of California, San Diego (UCSD) CMRR site or Eraser/DBAN a freeware tool that is readily available on the Internet.
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.  Degaussing is exposing the 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. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. <ul style="list-style-type: none"> <li>• <i>Disintegration or Pulverization.</i> These sanitization methods are designed to completely destroy the media.</li> <li>• <i>Shredding.</i> Paper shredders can 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 should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.</li> </ul> <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing or crosscut shredding.</p>

## 6.2 Sanitization Guidelines

The following table can be used to determine recommended sanitization of specific media. This recommendation should reflect the security categorization of the media to reduce the impact of harm of unauthorized disclosure of information from the media.

Not all types of available media are specified in this table. If your media is not included in this guide, you should identify and use processes that will fulfill the intent to clear, purge, or destroy your media.

**Media Sanitization Decision Matrix**

Media Type	Clear	Purge	Physical Destruction
<b>Hard Copy Storages</b>			
Paper and microforms	See Physical Destruction.	See Physical Destruction.	<ul style="list-style-type: none"> <li>Destroy paper using cross cut shredders or pulverize.</li> <li>Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) cross cut shredders or pulverize.</li> </ul>
<b>Hand-Held Devices</b>			
Cell Phones	<p>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.</p> <p>Contact the manufacturer for proper sanitization procedure.</p>	Same as Clear.	<ul style="list-style-type: none"> <li>Disintegrate.</li> <li>Pulverize.</li> </ul>
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	<p>Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state.</p> <p>Contact the manufacturer for proper sanitization procedure.</p>	Same as Clear.	<ul style="list-style-type: none"> <li>Pulverize.</li> </ul>
<b>Networking Devices</b>			

Routers (home, home office, enterprise)	<p>Perform a full manufacturer's reset to reset the router back to its factory default settings.</p> <p>Contact the manufacturer for proper sanitization procedure.</p>	Same as Clear.	<ul style="list-style-type: none"> <li>Disintegrate.</li> <li>Pulverize.</li> </ul>
<b>Equipment</b>			
Copy Machines	<p>Perform a full manufacturer's reset to reset the copy machine to its factory default settings.</p> <p>Contact the manufacturer for proper sanitization procedure.</p>	Same as Clear.	<ul style="list-style-type: none"> <li>Disintegrate.</li> <li>Pulverize.</li> </ul>
Fax Machines	<p>Perform a full manufacturer's reset to reset the fax machine to its factory default settings.</p> <p>Contact the manufacturer for proper sanitization procedures.</p>	Same as Clear.	<ul style="list-style-type: none"> <li>Disintegrate.</li> <li>Pulverize.</li> </ul>
<b>Magnetic Disks</b>			
Floppies	Overwrite media by using approved software and validate the overwritten data.	Degauss	<ul style="list-style-type: none"> <li>Shred.</li> </ul>
ATA Hard Drives	Overwrite media by using approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> <li>Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site.</li> <li>Purge hard disk drives by either purging the hard disk drive in an automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with a degaussing wand. Degaussing any current generation hard disk will render the drive <u>permanently</u> unusable.</li> </ol>	<ul style="list-style-type: none"> <li>Disintegrate.</li> <li>Pulverize.</li> </ul>

<p>USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives</p>	<p>Overwrite media by using approved and validated overwriting technologies/methods/tools.</p>	<p>1. Purge using Secure Erase The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site or Eraser.</p> <p>2. Purge hard disk drives by either purging the hard disk drive in an approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an approved degaussing wand. Degaussing any current generation hard disk will render the drive <u>permanently unusable</u>.</p>	<ul style="list-style-type: none"> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>
<p>Zip Disks</p>	<p>Overwrite media by using approved and validated overwriting technologies/methods/tools.</p>	<p>Degauss using an approved degausser. Degaussing any current generation zip disks will render the disk <u>permanently unusable</u>.</p>	<ul style="list-style-type: none"> <li>• Shred.</li> </ul>
<p>SCSI Drives</p>	<p>Overwrite media by using approved and validated overwriting technologies/methods/tools.</p>	<p>Purge hard disk drives by either purging the hard disk drive in an approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an approved degaussing wand.</p> <p>Degaussing any current generation hard disk will render the drive <u>permanently unusable</u>.</p>	<ul style="list-style-type: none"> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>

<b>Magnetic Tapes</b>			
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. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.</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.</p>	<ul style="list-style-type: none"> <li>• Shred.</li> </ul>
<b>Optical Disks</b>			
CDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <ul style="list-style-type: none"> <li>• Removing the Information bearing layers of CD media using a commercial optical disk grinding device.</li> <li>• Use optical disk media shredders or disintegrator devices.</li> </ul>
DVDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <ul style="list-style-type: none"> <li>• Removing the Information bearing layers of DVD media using a commercial optical disk grinding device.</li> <li>• Use optical disk media shredders or disintegrator devices to reduce DVD into particles.</li> </ul>
<b>Memory</b>			
Compact Flash Drives, SD	Overwrite media by using approved and validated overwriting technologies/methods/tools.	See Physical Destruction.	<p>Destroy media in order of recommendations.</p> <ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>

Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's data sheets.	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred</li> <li>• Disintegrate</li> <li>• Pulverize</li> </ul>
Electronically Erasable PROM (EEPROM)	Overwrite media by using approved and validated overwriting technologies/methods/tools.	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> <li>• Incinerate by burning in a licensed incinerator.</li> </ul>
Erasable Programmable ROM (EPROM)	<p>Clear media in order of recommendations.</p> <ol style="list-style-type: none"> <li>1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations</li> <li>2. Overwrite media by using approved and validated overwriting technologies/methods/tools.</li> </ol>	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> <li>• Incinerate by burning in a licensed incinerator.</li> </ul>
Flash Cards	Overwrite media by using agency approved and validated overwriting technologies/methods/tools.	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>
Flash EPROM (FEPROM)	Perform a full chip purge as per manufacturer's data sheets.	<p>Purge media in order of recommendations.</p> <ol style="list-style-type: none"> <li>1. Overwrite media by using approved and validated overwriting technologies/methods/tools.</li> <li>2. Perform a full chip purge as per manufacturer's data sheets.</li> </ol>	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> <li>• Incinerate by burning in a licensed incinerator.</li> </ul>
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 a disintegrator to reduce the card's internal circuit board and components to particles.
RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>

ROM	See Physical Destruction.	See Physical Destruction.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using approved and validated overwriting technologies/methods/tools	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> </ul>
Smart Cards	See Physical Destruction.	See Physical Destruction.	<p>For smart card devices&amp; data storage tokens or cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder.</p> <p>Smart that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration.</p>

## 7.0 Enforcement

Any person found in violation of Federal, State law or University policy, regulation or procedures is subject to loss of privileges, disciplinary action, personal liability and /or criminal prosecution. The University may block access to or remove a network connection that is endangering computing and or network resources or that is being used for inappropriate or illegal use. Information Technology will work with the Dean of Students, the UNC Police the academic deans and directors and others to enforce this policy.

## 8.0 Related Policies, Procedures, and Codes of Conduct.

All applicable laws and University policies, regulations and procedures bind UNC students and employees.

- [UNC Acceptable User Regulation](#)
- [Sensitive and Protected Data Management](#)