

IT Security

Information Technology Systems and Services

UND Computer Surplus, Transfer, and Disposal Procedures

Table of contents

- I. Transferring Computer Systems
- II. Surplusing and Disposing of Computer Systems
- III. Trade-in or Leased Computer Systems
- IV. Destruction Procedures
- V. Secure Erase Procedures
- VI. Block Overwrite Procedures
- VII. Macintosh Disk Erase Procedures
- VIII. Related Documents/Policies
- IX. Effective Dates
- X. Contacts

I. Transferring Computer Systems

These procedures should be followed for all computers prior to following the procedures in II. Surplusing and Disposing of Computer Systems.

- a. ITSS has developed a [Computer Transfer website and procedures](#) to assist departments in transferring and locating available computers. These procedures should be followed for those wishing to transfer their computer to another department.
- b. Prior to transfer, the transferring department must verify all records are transferred off of the computer system and retained in accordance with the UND Records Retention Schedule.
- c. Prior to transfer, the transferring department must sanitize the hard drive in the computer using one of the following methods.
 - i. Level 1: Destruction – This can be done at the discretion of the department if the risk associated with sanitizing at a lower level would be too great, typically because of the amount or type of confidential information on the computer. This should also be performed on hard drives that are damaged or otherwise unwritable. The receiving department would be responsible for replacing the hard drive if this option is chosen. [Refer to the destruction procedures \(Section IV\) for more information.](#)
 - ii. Level 2: Secure Erase – This is the minimum requirement for all computers whose hard drives are compatible with this technique. This sanitation method is accomplished by running a Secure Erasure utility which executes the Secure Erase command on the firmware of the disk drive. This command is implemented in all recent ATA drives greater than 15-20GB. [Refer to the Secure Erase procedures \(Section V\) for more information.](#)
 - iii. Level 3: Block Overwrite – This is required of all computers whose drives do not support the Secure Erase command. This would include SCSI drives or ATA drives manufactured prior to 2001 (typically, drives smaller than 15GB). [Refer to the Block Overwrite procedures \(Section VI\) for more information.](#)

- iv. Level 4: Imaging or Formatting – This level of sanitation is only acceptable for computers originating in labs or student areas where it is known that no confidential information is present.

II. Surplusing and Disposing of Computer Systems

Prior to surplusing or disposing of a computer system, please follow the procedures in section I. to see if your computer can be transferred to another department. If it cannot be used by another department and you wish to dispose of the computer, please follow the below procedures. All computers must be disposed of through the UND Facilities Surplus Property Department.

- a. Prior to disposal, the transferring department must verify all records are transferred off of the computer system and retained in accordance with the UND Records Retention Schedule.
- b. Before the computer is disposed of, the transferring department has the option of whether or not they will sanitize the hard drive. A department may want to sanitize as an extra precaution, but once the computer is transferred to Surplus Property, they will follow internal [procedures](#) to ensure proper destruction and disposal of hard drives.
- c. If the transferring department chooses to sanitize the hard drive, one of the following methods should be used.
 - i. Level 1: Destruction – This can be done at the discretion of the department if the risk associated with sanitizing at a lower level would be too great, typically because of the amount or type of confidential information on the computer. [Refer to the destruction procedures \(Section IV\) for more information.](#)
 - ii. Level 2: Secure Erase – This sanitation method is accomplished by running a Secure Erasure utility which executes the Secure Erase command on the firmware of the disk drive. This command is implemented in all recent ATA drives greater than 15-20GB. [Refer to the Secure Erase procedures \(Section V\) for more information.](#)
 - iii. Level 3: Block Overwrite – This would be used for computers whose drives do not support the Secure Erase command. This would include SCSI drives or ATA drives manufactured prior to 2001 (typically, drives smaller than 15GB). [Refer to the Block Overwrite procedures \(Section VI\) for more information.](#)
 - iv. Level 4: Imaging or Formatting – This level of sanitation is only acceptable for computers originating in labs or student areas where it is known that no confidential information is present.
- d. Once the sanitation is complete, or if the department chooses not to sanitize, the department should send the computer(s) to Surplus Property by following the [UND Surplus Property Procedures](#)
- e. Surplus Property will follow internal [procedures](#) to ensure proper handling and accounting of computer systems and proper destruction of hard drives.

III. Trade-in or Leased Computer Systems

If the computer is leased or will be traded-in to a manufacturer for a new computer, the transferring organization must follow the following procedures prior to trading-in or returning the leased computer.

- a. Prior to trading-in or returning a leased computer, the transferring department must verify all records are transferred off of the computer system and retained in accordance with the UND Records Retention Schedule.
- b. Prior to trading-in or returning a leased computer, the transferring department is responsible for making sure the hard drive is sanitized using one of the following methods.
 - i. Level 1: Destruction – This can be done at the discretion of the department if the risk associated with sanitizing at a lower level would be too great, typically because of the amount or type of confidential information on the computer. This should also be performed on hard drives that are damaged or otherwise unwritable. For leased computers, destruction of the hard drive may not be possible due to the lease agreement. [Refer to the destruction procedures \(Section IV\) for more information.](#)
 - ii. Level 2: Secure Erase – This is the minimum requirement for all computers whose hard drives are compatible with this technique. This sanitation method is accomplished by running a Secure Erasure utility which executes the Secure Erase command on the firmware of the disk drive. This command is implemented in all recent ATA drives greater than 15-20GB. [Refer to the Secure Erase procedures \(Section V\) for more information.](#)
 - iii. Level 3: Block Overwrite – This is required of all computers whose drives do not support the Secure Erase command. This would include SCSI drives or ATA drives manufactured prior to 2001 (typically, drives smaller than 15GB). [Refer to the Block Overwrite procedures \(Section VI\) for more information.](#)
 - iv. Level 4: Imaging or Formatting – This level of sanitation not acceptable for trade-in or leased computers.

IV. Destruction Procedures

Destruction of hard drives is the ultimate form of sanitization. After hard drives are destroyed, they cannot be reused as originally intended. Destruction should be used if the drive will be sent out of the control of the University (other than trade-in or leased computers), if the information on the drive has high-risk confidential information, or if the drive is damaged or otherwise not re-writable.

- a. Prior to destruction, the transferring department must verify all records are transferred off of the computer system and retained in accordance with the UND Records Retention Schedule.
- b. The department seeking destruction should make a record of all drives sent to be destroyed noting at minimum the serial number of the drive, the date of destruction, and the individual or organization conducting the destruction. This record should be kept with the office of record pursuant to the records retention schedule.
- c. Physical destruction should be accomplished using one of the following methods. For those that do not have the in-house capability to destroy using one of the following methods, the department should follow the [UND Surplus Property Procedures](#) to send the drive to Surplus Property for destruction.
 - i. Disintegration - the act of separating into component parts.
 - ii. Incineration – the act of burning completely to ashes
 - iii. Pulverizing – the act of grinding to a powder or dust
 - iv. Shredding – the act of cutting or tearing into small particles

- v. Melting – to be changed from a solid to a liquid state generally by the application of heat

V. Secure Erase Procedures

Secure Erase is an overwrite technology using a firmware based process to overwrite a hard drive. It 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 a block overwrite. ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command built in. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives. A program called hdderase.exe will be used to perform the secure erase. This program only works on SATA/ATA drives, and only detects drives on the primary and secondary IDE channels. If you have a SCSI drive, or a secondary drive which is not jumpered as a master or slave, the program may not detect your hard drive. Prior to wiping, you should always verify the hard drives installed in the computer and make sure to secure erase or block overwrite each drive.

- a. Download the boot CD iso image available [here](#).
- b. Burn the image to a CD using your favorite CD burning application. Most applications, such as Roxio Creator, will have an option or capability to burn an iso image to CD. If you need assistance, contact the IT Security Officer.
- c. Boot the computer from the CD. You may have to change the boot priority settings in your BIOS to boot from the CD.
 - Note:** For laptop users, please make sure that there is sufficient battery life to run and complete the secure erase procedure. Secure erase may take as long as three hours for larger capacity drives. If power is lost during the secure erase, the drive will be locked and the secure erase will have to be run again until it completes.
- d. From the Main menu of the Boot CD, select **Hard Disk Tools** and hit enter.
- e. Select **Wiping Tools** and hit enter.
- f. Select **HDDERASE V4.0** (or current version) and hit enter.
- g. Answer Y when prompted with DO YOU WANT TO PROCEED?
- h. “Press any key” to continue after reviewing the license agreement
- i. Press Y when shown the license agreement and asked: Do you agree?
- j. Answer Y when prompted with DO YOU WANT TO PROCEED?
- k. Enter your selection for which drive to secure erase (i.e. P0)
- l. Press Y when asked: This drive supports the ATA security feature set, do you want to proceed to the options menu? If the drive does not support the security feature set, you will need to block overwrite the drive by following the procedures in section VI.
- m. You may now receive a message that states “ATA security feature set is prohibited by the system BIOS chip. Do you want HDDERASE to attempt to override the BIOS?” Press Y and reboot the system. You will have to again walk through the procedures above, but you should no longer receive this message. If you do, see the [HDDERASE readme FAQ](#) for other ways to bypass the BIOS, otherwise you will have to block overwrite the drive by following the procedures in section VI.
- n. At the options menu, when prompted with: “Please enter your selection,” enter 1 for executing secure erase and hit enter.
- o. Press Y and hit enter when asked: Do you want to proceed?
 - Note:** This uses the ATA internal drive secure erase command. It offers a higher level of secure erase than block overwriting software utilities. It can take 30 to 180 minutes depending on the drive’s capacity and speed (the program will display the

- estimated duration for the secure erase process while executing). The drive will be left unlocked and ready for use once the process has successfully completed.
- p. When the secure erase is finished, select the option to view the audit log, and document the Serial Number of the hard drive for your records.

VI. Block Overwrite Procedures

- a. Follow these procedures if:
 - i. You followed the procedures in section V. and could not run the Secure Erase option (either it wasn't available or you were unable to run it)
 - ii. You have a SCSI hard drive
- b. If you haven't done so already, download the boot CD iso image available [here](#).
- c. Burn the image to a CD using your favorite CD burning application. Most applications, such as Roxio Creator, will have an option or capability to burn an iso image to CD. If you need assistance, contact the IT Security Officer.
- d. Boot the computer from the CD. You may have to change the boot priority settings in your BIOS to boot from the CD.
- e. From the Main menu of the Boot CD, select **Hard Disk Tools** and hit enter.
- f. Select **Wiping Tools** and hit enter.
- g. Select **Darik's Boot and Nuke V1.0.7** (or latest version) and hit enter.
- h. If you desire, you can hit the **M** key and change the Wipe Method.
- i. Next, use the arrow keys and press the space bar to select the hard drive(s), and press **F10** to start the overwrite procedures.

VII. Macintosh Disk Erase Procedures

This procedure will work for Mac's with OS X 10.3.x and higher and uses the Macintosh Disk Utility on the OS X system CD that came with your Macintosh. If you do not have a system disk or have a Mac with an OS later than OSX 10.3.x, contact the IT Security Officer.

- a. Insert the CD into the CD drive, and hold down the C key during the startup process
- b. Select your preferred language. You will then see the **Welcome to the Mac OS X Installer** window.
- c. From the **Installer Menu Bar**, click **Open Disk Utility**. You will then see the **Disk Utility** window.
- d. In the left pane of the **Disk Utility** window, click the drive you want to erase.
- e. In the right pane of the Disk Utility window, click the Erase tab.
- f. From the Volume Format drop-down menu, select Mac OS Extended (Journaled).
- g. In the Name field, highlight the existing text and type the name the hard drive is to be called after it's formatted.
- h. The following are the available security options:
 - **Don't Erase Data**
 - **Zero Out Data**
 - **7-Pass Erase**
 - **35-Pass Erase**
- i. Click the radio button in front of **7-Pass Erase**
- j. Click **OK**.
- k. Click **Erase**.

1. Confirm you want to erase. The program will unmount the volume, partition the drive, and rename the volume to the name you typed in step g above.

VIII. Related Documents/Policies

- [UND Surplus, Transfer, and Disposal Policy](#)
- [ITSS Computer Transfer Website](#)
- [UND Records Retention Schedule](#)
- [UND Surplus Property Policy](#)

IX. Effective Dates

Last Modified: March 31, 2009

Effective: October 15, 2009

X. Contacts

Contact	Phone
UND IT Security Officer	777-3587
UND Surplus Property	777-3125