

# IT Security

Information Technology Systems and Services

## UND Computer Surplus, Transfer, and Disposal Policy

---

### Table of contents

- I. Reason for the Policy
  - II. Applicability of the Policy
  - III. Policy Statement
  - IV. Definitions
  - V. Related Documents / Policies
  - VI. Effective Dates
  - VII. Contacts
- 

### I. Reason for the Policy

The surplusing, transferring, trade-in, and disposal of computers can create information security risks for the University. These risks include, but are not limited to, the unauthorized release of confidential information, the violation of software license agreements, and the unauthorized disclosure of intellectual property that might be stored on the hard drives. This policy will outline the necessary requirements for individuals and departments to follow in order to limit these risks.

---

### II. Applicability of the Policy

This policy applies to all members of the University community who are responsible for surplusing, transferring, trading-in, or disposing of University-owned or leased computer systems.

---

### III. Policy Statement

#### **A. Surplusing and Disposing of Computer Systems**

All computers to be surplused or disposed of must be transferred to the UND Facilities Surplus Property Department in accordance with the UND Surplus Property Policy.

Although not required, the department surplusing the computer may decide to remove confidential data from the computer prior to sending it to the UND Surplus Property Department. Data removal may be performed according to any of the four levels of sanitation discussed in section B. Transferring Computer Systems.

The UND Facilities Surplus Property Department will ensure that computers it receives for surplus are processed so that the hard drives are properly destroyed. The UND Facilities Department staff may destroy the hard drives, or they may contract with a 3rd party for destruction. The Information Technology Security Officer (ITSO) will provide guidance and review destruction practices to ensure they meet the standards of this policy.

#### **B. Transferring Computer Systems**

When transferring a computer to another department on campus, or within a department, it is the responsibility of the transferring department to sanitize the drive by removing licensed software and/or confidential data from the hard drive prior to transfer.

Sanitation will be done according to the following levels:

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.

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.

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).

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.

### **C. Trade-in or Leased Computer Systems**

When returning a leased computer or trading-in a computer, the department conducting the trade-in or returning the leased computer is responsible for ensuring all data is removed from the hard drive using a Level 1, 2 or 3 sanitation method as discussed in section B. Transferring Computer Systems. Level 4 sanitation is not acceptable for trade-in or leased computers.

### **D. Records Retention**

Prior to surplus, transferring, or trading-in a University owned computer, or returning a leased computer, it is the responsibility of the system owner and owning department to verify all records are transferred off of the computer system and retained in accordance with the UND Records Retention Schedule.

---

## **IV. Definitions**

*Confidential Information* Information that UND is under legal or contractual obligation to protect or information that is not to be publicly disclosed. The disclosure, use, or destruction of this type of information can have adverse affects on UND and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information such as open legal investigations conducted by the Institution, sealed bids, trade secrets, intellectual property, research activities, social security numbers, passwords, location of assets, donors, student information, etc.

*Destruction* The result of actions taken to ensure that hard drives cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive. Acceptable techniques include disintegration, pulverization, melting, incineration, and shredding.

<i>Secure Erase</i>	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 3-pass 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.
<i>Block Overwrite</i>	Writing patterns of data on top of the data stored on a hard drive. This technique typically uses software or hardware products to overwrite storage space on the hard drive 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. Overwriting cannot be used for hard drives that are damaged or not rewriteable.
<i>Imaging</i>	Copying of the contents of a computer's hard drive into a single compressed file or set of files (referred to as an <i>image</i> ) so that the contents of the hard drive, including configuration information and applications, can be copied to the hard drive of another computer. This process will automatically format and partition the target hard drive, and often can be done so that it overwrites much or all of the data on the target drive. A software application typically used for this is Norton Ghost, a product by Symantec.
<i>Formatting</i>	A process performed by an operating system to prepare a hard drive for reading and writing. The operating system will erase all bookkeeping information on the disk drive, test the disk to make sure all sectors are reliable, mark bad sectors, and create internal address tables that it later uses to locate information. Note that reformatting a disk does not erase the data on the disk, only the address tables; therefore, the data may still be recovered using specialized software and/or hardware.

---

## V. Related Documents / Policies

- NDUS 1901.2 Data Classification and Information Technology Security Standards
  - <http://www.ndus.nodak.edu/uploads/document-library/1620/P-1901.2-DATA.STD.12-14-2007.PDF>
- UND Computer Surplus, Transfer, and Disposal Procedures
  - <http://itsecurity.und.edu/ComputerDisposal/ComputerDisposalProcedures.html>
- UND Surplus Property Policy
  - <http://www.und.edu/dept/policyoffice/Policies/facilities/PDF/5.2%20surplus%20property%20-%2012.16.08.pdf>
- UND Records Retention Schedule
  - <http://www.und.edu/dept/records/forms/UNDRRS.pdf>
- North Dakota State Surplus Property Computer Disposal Policy
  - <http://www.nd.gov/surplus/computer.htm>
- National Institute of Standards and Technology (NIST) Special Publication 800-88
  - [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)

---

**VI. Effective Dates**

Last Modified: March 31, 2009

Effective: October 15, 2009

Next Review Date: October 15, 2011

---

**VII. Contacts**

<b>Subject</b>	<b>Contact</b>	<b>Phone</b>
Information Security	UND IT Security Officer	777-3587
Records Retention	Records Manager	777-6797
Surplus Property	UND Facilities Surplus Property	777-3125

DRAFT