

Approved: March 14, 2007

**University of Massachusetts**  
**Standards for the Redistribution and Disposition of Computer Equipment and**  
**Electronic Storage Devices**

## **I. PURPOSE**

These Standards are issued pursuant to the Board of Trustees' [Capitalization and Inventory Control Policy \(Doc. T96-073\)](#) adopted June 5, 1996) and are being established to ensure compliance with federal and state statutes associated with confidential/private information, (i.e., [Health Information Portability and Accountability Act of 1996](#) – HIPAA, [Family Educational Rights and Privacy Act](#) –FERPA, etc.), to ensure proper disposal of materials in an environmentally safe method, to protect University data and/or intellectual property from inadvertent disclosure, and to ensure the rights of privacy of University staff and students.

## **II. SCOPE**

These Standards:

- a. Are based on the laws of the Commonwealth of Massachusetts, the United States and other regulatory agencies. Policies, guidelines/standards and procedures may impose certain restrictions that are not specifically covered by state and federal law, or other regulations.
- b. Shall not be construed to be inconsistent with any contractual obligation of the University.
- c. Apply to all computer equipment and electronic devices (e.g., hard-drives, zip drives, flash drives, laptops, servers, mainframes, personal digital assistants, handheld computers, keyboards, printers, scanners, fax machines, monitors, power supplies, chips, cables, network cards, magnetic or optical media, etc.) owned by the University of Massachusetts (i.e., University) regardless of their location (e.g., on University premises, on loan with staff, etc.)
- d. Apply to all employees of the University.
- e. Function in conjunction with other [University data and computing policies, guideline/standards, procedures](#) and campus procedures.

### **General**

Department's using computer hardware and electronic storage devices are the custodians (i.e., custodial department) of this equipment.

Custodial departments are responsible for ensuring that all computer hardware and electronic storage devices under their area of responsibility are properly handled and secured from the point of delivery to the time of disposal.

Approved: March 14, 2007

Based on Massachusetts laws and University policy, surplus or obsolete computer hardware and electronic storage devices can be disposed of in different methods depending on the use of the equipment and the source of funding used to purchase the item:

- All surplus or obsolete computer hardware and electronic storage devices can be traded in for new equipment.
- If the computer hardware or electronic storage devices were purchased as educational or scientific equipment, the University has no restrictions (except for proper environmental handling if item is destroyed) regarding how these items are disposed of regardless of the source of funding.
- If the computer hardware or electronic storage devices were purchased for purposes other than as educational or scientific equipment (e.g., University departments to perform University business), the source of funding determines how the items may be disposed of:

<b>Source Of Funding</b>	<b>Transfer To Another University Department</b>	<b>Transfer To State Agency Or State Surplus</b>	<b>Donate Or Sell To External Organizations, Staff/Students, Or The General Public</b>	<b>Recycle/Destroy</b>
State (must follow state surplus regulations for disposal)	X	X		X
Trust	X		X	X
Grant	*	*	*	*

\*Computer hardware and electronic storage devices purchased via grant funds must be disposed of based on restrictions noted in the grant contract. If no restrictions are noted, these items are considered University property with no disposal restrictions (except for proper environmental handling if item is destroyed) in effect.

If the custodial department is unsure of the funding source of the computer hardware or electronic storage devices, it should be deemed state property and handled appropriately.

Any software and/or data files left on a hard drive, mainframe, server, and/or electronic storage device can potentially be retrieved. This can lead to violations of software license agreements, result in unauthorized access to University data, and/or violate state and federal data security and privacy laws. It is critical therefore, to properly remove data and licensed software from any computer hardware or electronic storage device that is being transferred to another entity or salvaged.

Approved: March 14, 2007

Departments transferring, donating, selling or salvaging/destroying computer hardware and/or electronic storage devices shall follow the requirements stated in this Standard in addition to any campus procedures related to equipment transfer, donation, sales or recycling/destruction. If campus procedures and this Standard conflict, this Standard takes precedent.

Written documentation shall exist for all transferred, donated, sold or recycled/destroyed computer hardware and electronic storage devices. The Official Records Custodian for this documentation shall be the department responsible for inventorying equipment at the applicable campus or President's Office. Such documentation shall be retained for 7 years and shall include:

- Name of Custodial Department
- Department Head Name and signature of Custodial Department
- Name of Accepting Department or Organization
- Accepting Department/Organization Head Name
- Date of Transfer, donation, recycling or destruction
- Date of Relocation to central repository, if to be sold or held in storage
- Condition of unit (i.e., functioning or not functioning)
- Description of computer hardware or electronic storage devices including manufacturer, model, location prior to disposition, University Inventory Tag number, and equipment serial number
- Cost and source of funding of unit, if known
- Statement noting that the software and data files have been electronically purged in compliance with these Standards followed by the name and signature of the individual attesting to the purge.
- Statement noting that equipment has been destroyed in compliance with these Standards, when applicable, followed by the name and signature of the individual attesting to the destruction.
- Statement noting that the computer hardware or electronic device was sold in compliance with state law and University policy, date item sold, and name and signature of individual attesting to sale (if applicable) and individual to whom the equipment was sold.

### **Equipment Software/Data Wiping**

Custodial departments shall, prior to computer hardware or electronic storage devices being transferred, donated, sold, recycled or destroyed shall:

- Migrate files contained on hardware or electronic storage devices that are **not** past their retention period to current systems or another suitable storage format.
- "Wipe"/Sanitize or contract another entity (e.g., another campus department such as IT, MHEC vendor, etc) to wipe/sanitize functioning hard-drives. Normal DOS programs such as "Delete", "Format" and "Fdisk" are **not** sufficient. These programs do not actually remove or write over the media. When

Approved: March 14, 2007

wiping/sanitizing computer hardware and electronic storage devices, custodial departments/contracted entities must use programs that comply with the Department of Defense (i.e., DoD) 5220.22-M disk overwriting standard which requires that every addressable location on the disk is overwritten by a single character. Prior to running such a program, departments/contracted entities shall have a disk or CD to boot the computer so that they can sanitize the entire hard-drive. Campus information technology units shall compile a list of approved wiping/sanitizing tools for their campus.

- Sanitize or contract another entity to sanitize floppy disks, tapes, CDs, DVDs, optical disks, etc. that may have Confidential data stored on them. If the custodial department is not sure if the medium contains such information, the medium shall be sanitized to ensure no sensitive data may be disclosed.
- Sanitize or contract another entity to sanitize nonvolatile memory components (i.e., memory components that retain data when all power sources are discontinued) including Read Only Memory (i.e., ROM), programmable ROM (i.e., PROM), or erasable PROM and their variants. Memory components that have been programmed at the vendor's facility and are considered unalterable can be transferred, salvaged or destroyed without being sanitized.

### **Salvaged Computer Equipment**

Computer hardware and electronic storage devices (functioning or nonfunctioning) shall not be placed in any trash receptacle, refuse dumpster, trash compactor or roll-off container. These materials generally contain significant quantities of lead, heavy metals, and other toxic material and are banned from landfill disposal. Severe legal and environmental consequences can result from improper disposal.

Campuses shall have a single, secure site to accumulate computer hardware and electronic devices waiting recycling or destruction. Computer equipment recycling and/or destruction may be performed by the campuses or a contracted service as long as the destruction of equipment is certified.

In addition to "wiping"/sanitizing functional computer drives (see Equipment Software/Data Purging section above), all hard-drives (functioning and nonfunctioning: standalone units, in computers or in other equipment slated to be recycled/destroyed) must be physically removed and destroyed. Hard-drives containing "Confidential" data should not be specially marked. This would call special attention to their value and make them a target for theft.

Physical destruction of hard-drives shall not be performed by a department.

Hard-drives may be dismantled and have the individual platters bent or destroyed. It may also have the spindle "punched" via mechanical or hydraulic equipment, or cut in half.

Approved: March 14, 2007

Drilling holes with a drill press or “smashing” on the ground are **not** approved or suggested methods of destruction.

Use of a degausser to destroy hard-drives is permitted only if it is a unit specifically designed for the purpose of degaussing modern hard-drives and should be capable of generating a magnetic field in excess of 4000 Gauss. These units are generally referred to as “Type I or Type II” degaussers. Degaussing will render a hard-drive permanently inoperable. Light duty degaussers designed for erasing floppy disks and audio tapes are not powerful enough to erase hard-drives or high density tapes such as DAT and DLT.

Any department which improperly disposes of computer or other equipment still containing hard-drives will be contacted by the appropriate CIO who will take appropriate action to correct their procedures.

If any computer hardware/electronic storage devices surplused for transfer to a UMass or state agency, donation or sale, or scheduled to be recycled/destroyed are found to contain:

- Data, the equipment’s custodian department will be charged for the audit and special handling costs which equal \$100.00 per unit.
- Patient health information, the equipment’s custodian department will be charged for the audit and special handling costs which equal \$100.00 per unit, and the name of the signer on the transfer form will be forwarded to the appropriate office as required under HIPAA.