

ITEM 131-107-R0506

Approval of University System Computer Disposal Policy

THAT:

The Board of Regents of Higher Education approves the new policy on appropriate disposal of computers and electronic storage devices.

EXPLANATION:

The State of Montana recently adopted a policy for all state agencies to follow regarding appropriate procedures for disposal or transfer of any state-owned computers or electronic storage devices. This state policy was developed in response to several incidents in which potentially sensitive data was present on computers disposed of by state agencies. IT professionals from both UM and MSU agreed that it would be difficult for the MUS to implement the state policy precisely as written, but the principal of having a uniform policy for the MUS was sound.

The MUS disposes of thousands of computers and storage devices (including CDs, disks, and other external storage medium) each year. Many computers are donated (to local K-12 schools, for example) and others are discarded. Each campus has its own procedures for ensuring sensitive information is removed from data storage devices (e.g. hard drives) prior to disposition. While campus level policies provide flexibility, they also lead to some inconsistencies that increase the potential for inadvertent dissemination of sensitive information, particularly with regard to protected student data.

The proposed policy was developed jointly by the Commissioner's Office, MSU and UM. It has as its foundation the policy developed for state agencies, but has been modified to allow for better implementation by the MUS. The team that developed this policy also believes this MUS policy provides slightly better safeguards than the state agency policy.

ITEM 131-107-R0506

**MONTANA BOARD OF REGENTS OF HIGHER EDUCATION
Policy and Procedures Manual**

SUBJECT: INFORMATION TECHNOLOGY

Policy 1308 – Disposal of Computer Storage Devices (New)

Effective _____; Issued _____

SCOPE

This policy applies to all campuses of the Montana University System including the Office of the Commissioner of Higher Education and to all departments, offices, and employees thereof. It addresses disposal of electronic information storage devices owned by campuses of the Montana University System, including those contained within or attached to personal computers, servers, laptops, PDAs, or any other computing devices, accessory equipment, or stand alone devices that store electronic data, information, and/or software programs.

This policy does not apply to electronic information storage devices, as described above, that are used by a campus of the Montana University System but are owned by a contractor, granting agency, service provider, or other entity that is external to the Montana University System, or is used exclusively for the purpose of supporting grant- or contract-related activities where the granting agency or contractor retains ownership of data associated with the activity.

PURPOSE

When information technology (IT) equipment is in normal use, it is assumed that the entity to which the equipment is assigned (the “Owner”) is responsible for guaranteeing appropriate security for all information stored on or maintained by that equipment. When the owner wishes to dispose of that equipment, explicit action must be taken to assure that confidential information does not remain accessible to a new owner. The responsibility of assuring that information security is maintained during disposal ultimately falls to the chief executive officer of the campus where the equipment is located but may, at the CEO’s discretion, be delegated to the original owner, a central campus authority such as the campus IT department, or to a specific individual. For purposes of this policy, the party to whom the campus CEO assigns this operational responsibility for assuring information security will hereinafter be called the “Responsible Party.”

Sensitive information includes data required by federal or state law to be protected from disclosure to individuals and entities both inside and outside of the Montana University System. For purposes of this policy, sensitive information also includes proprietary software that is licensed to campuses of the Montana University System, which must be protected against unauthorized distribution.

This policy outlines disposal requirements for protecting these IT assets by either of two methods: (1) destruction of the IT device; or, (2) complete removal of all electronic data from the computer storage device. The responsible party must perform at least one of these actions before disposing of the device.

DEFINITIONS

Owner	The MUS department, division, or other administrative unit that is directly responsible for the management and maintenance of the computer and/or computer storage device or media.
Disposal	An authorized change of ownership for an IT storage device -- the original owner disposes of the device and gives up responsibility; a new owner obtains the device and accepts responsibility. As a special case the device is destroyed -- there is no new owner and responsibility for management ceases.
Computer Storage Device	Includes, but is not limited to: personal computers with hard drives, servers with hard drives, other assets with hard drives or loose/unattached hard drives.
Cleaning or Cleaned	A process used to assure that data is destroyed or removed from an IT storage device. This may be achieved by physical destruction of the device or by the proper use of specialized software utility programs that overwrite the data so that it is unrecoverable. Note: This cleaning process is also known as a "sanitizing" or "scrubbing" process.
Removable storage Media	Includes, but is not limited to: floppy diskettes, compact disks (CD's), magnetic tapes, digital video devices (DVD's), Zip media, Flash media, and all other similar removable media.
Physical Destruction	To incinerate, pulverize, shred, or melt or otherwise destroy the computer storage device, removable storage media, or component so as to render it incapable of storing or retrieving electronic data or software programs.

DISPOSAL REQUIREMENTS

All computer storage devices and removable storage media must be cleaned prior to disposal, regardless of how their owner chooses to dispose of them. This includes but is not limited to internal transfers, transfers between campuses and/or state agencies, disposal through standard surplus equipment processes, and donation to a public school or to the Office of Public Instruction. Owners disposing equipment through the state Property and Supply Bureau's surplus equipment program should contact their campus property management office or the Property and Supply Bureau for any additional requirements.

The owner must work with the Responsible Party designated for that campus to assure that disposal conforms to the following requirements.

1. All data maintained specifically by the owner and any software programs that are licensed exclusively to the owner must be removed from storage devices and/or media prior to their disposal, except that legally licensed operating system software (e.g., Microsoft Windows) that is tied to a specific computer serial number and which may be legally transferred with the computer to another licensee, may remain on (or may be restored to) the storage device following the cleaning process. (Note: Because of the varying circumstances under which computers may have been acquired, it is the responsibility of the owner to determine, prior to transferring any licensed operating system software, whether it is legally permissible to do so.)
2. Alternatively, if data and/or software programs contained on the storage device and/or media cannot be removed according to the following process, then that device and/or media must be destroyed.
3. To remove data and software from rewritable storage devices or media, the Responsible Party must use a Department of Defense (DoD) 5220.22-compliant sanitation program or an equivalent

method of removal or destruction of data and software (such as high-intensity degaussing of magnetic storage media) that will effectively sanitize the hard drive. To be DoD 5220.22-compliant, programs must use the DoD's "three-pass" process to: (1) overwrite all electronically addressable locations on the device with a character; (2) overwrite it again with the same character's complement bit configuration; and then (3) overwrite it again with a random character. Finally, the program must perform a verification process to assure that the cleaning has been accomplished.

Software products are available, both freeware and purchased, that comply with DoD requirements for storage cleaning. See the [State of Montana's software standards](http://www.discoveringmontana.com/itsd/policy/ByCategory.asp) at <<http://www.discoveringmontana.com/itsd/policy/ByCategory.asp>> for a list of acceptable products.

For more information from the DoD regarding the topic of Automated Information System Security, see the [Department of Defense three pass process](http://www.dtic.mil/whs/directives/corres/pdf/522022m_0195/cp8.pdf) at <http://www.dtic.mil/whs/directives/corres/pdf/522022m_0195/cp8.pdf>.

4. If the data storage device cannot be put through this process because it is not functional or because it is not rewritable, the device must be physically destroyed.
5. All removable storage media must be cleaned using a method such as high-intensity degaussing or must be physically destroyed.
6. The owner is responsible for maintaining documentation on all electronic data storage devices (e.g., PCs, laptops, servers, PDAs) that have been either destroyed or sanitized. The owner must retain these records for two years following disposal.

The disposal records shall contain the following information:

- a. Device identification (vendor serial number or equivalent)
- b. Date of cleaning
- c. Employee name performing cleaning
- d. Method of cleaning
- e. Destination/new owner of device (includes "destroyed/none")
- f. Responsible Party sign-off

IMPLEMENTATION

If the campus CEO has explicitly assigned a specific campus unit or person as the Responsible Party, an owner MUST transfer all computers and removable storage media to that Responsible Party for disposal, even if the final destination is another on-campus unit. In the absence of the explicit assignment of this responsibility to a specific unit or person, the owner retains full responsibility to clean computers and media before disposing of them in any manner.

BACKGROUND

This policy is based in large part on a similar policy created by the Information Technology Security Office of the Information Technology Services Division for the State of Montana. Information contained in this policy originated from the Section 1-0250.00, MOM.