UMBC POLICY ON ELECTRONIC MEDIA DISPOSAL
UMBC# X-1.00.05

I. POLICY STATEMENT

Increasing amounts of electronic data are being transmitted and stored on computer systems and electronic media by virtually every person conducting business for UMBC. Some of that data contains sensitive and/or proprietary information, including student records, personnel records, financial data, research data, intellectual property including unpublished research, protected health information and software. Software licensed to UMBC may not be transferable outside UMBC. If the information on those systems is not properly removed before the equipment is disposed of or transferred, that information could be accessed, viewed or used by unauthorized individuals.

As such, all users of computer systems within UMBC, including contractors and vendors with access to UMBC systems, are responsible for taking the appropriate steps, as outlined below to ensure that all computers and electronic media containing sensitive and/or proprietary information are properly sanitized before disposal or transfer Electronic Media is defined as any electronic storage device that is used to record information, including, but not limited to hard disks, external hard drives, magnetic tapes, compact disks (CD), digital video disks (DVD) videotapes, audiotapes, and removable storage devices such as floppy disks, zip disks and thumb drives.

II. PURPOSE FOR POLICY

The purpose of this policy is to establish a standard for the proper disposal and transfer of electronic media containing sensitive and/or proprietary data. The disposal procedures used will depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

III. ENTITIES AFFECTED BY THIS POLICY

All academic and administrative units of the UMBC community.

IV. WHO SHOULD READ THIS POLICY

A. Vice Presidents, Deans, Directors, and Department Heads
B. Department administrators and business office staff
C. Campus Senates, Steering Committee, and Standing Committees
D. Departmental IT Support Staff

V. CONTACTS

Direct any general questions about this University Policy – UMBC Policy Formulation and Management first to your department's administrative office. If you have specific questions, call the following offices:

Subject	Contact	Telephone / Email
Policy Clarification	Office of Information Technology	(410) 455-3208
Standard Format Information	UMBC Policy Liaison	(410) 455-2772

VI. DEFINITIONS

Electronic Media	Any electronic storage device that is used to record information, including, but not limited to hard disks, external hard drives, magnetic tapes, compact disks (CD), digital video disks (DVD) videotapes, audiotapes, and removable storage devices such as floppy disks, zip disks, magnetic stripes on cards and thumb drives.
Electronic Media (Other Than Hard Drives)	Electronic Media, *other than hard drives*, refers to any electronic storage device that is used to record information, including, but not limited to magnetic tapes, compact disks (CD), digital video disks (DVD) videotapes, audiotapes, and removable storage devices such as floppy disks, zip disks, magnetic stripes on cards, and thumb drives.
Sensitive Data	Sensitive and/or proprietary information, including student records, personnel records, financial data, research data, intellectual property including unpublished research, protected health information and software. Software licensed to UMBC that may not be transferable outside UMBC.
Clearing	Clearing information is a level of media sanitization that would protect confidentiality of information against a simple attack. Examples of this include, but are not limited to, a simple single pass format of the hard drive or deletion of data from removable media such as thumb drives. This level of sanitization does not prevent data from being retrieved using data recovery tools but it will prevent simple access to data.
Purging	Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack (e.g. advanced data recovery software/tools) and will render the data unreadable. *Example: For hard drives this may include the use of a hard drive wiping utility that repeatedly "writes" random data to the hard drive making data recovery impossible.* Purging can also be accomplished through the use of degaussing of magnetic storage materials (*e.g. hard drives and magnetic tapes*).

	Degaussing exposes magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. Generally, degaussing permanently renders the magnetic media unusable. *These processes should be performed in accordance with the NIST recommended standards.*
Destroying	Destruction of media is the ultimate form of sanitization. After the media are destroyed, they can not be reused as originally intended. Approved methods of destructions include *Shredding, Disintegration, Incineration, Pulverization and Melting.* The University encourages use of certified commercial disposal systems.

VII. UNIVERSITY POLICY

A. Hard Drives

Prior to disposal or transfer, hard drives must be ***Cleared, Purged*** or ***Destroyed*** in accordance with the methods described within this policy.

i. Transfer of Hard Drives

1. **Intradepartmental:** *Transfer of hard drives within a department.* Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Since the drive is remaining within the department, the hard drive may instead be ***Cleared*** prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the *UMBC Acceptable Use Policy*
2. **InterDepartmental:** *Transfer of hard drives to another department.* Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be ***Purged*** in a manner described above.

ii. Warranty Replacement of Hard Drives

Hard drives containing ***Sensitive*** data shall not be released from the UMBC owner's possession unless the data contained within the hard drive has been ***Purged*** or ***Destroyed*** in accordance with this policy.

iii. Recovery of Hard Drives

Sending a hard drive out for data recovery. The vendor recovering data on the hard drive must sign an appropriate contractual agreement, which must be approved by campus legal, insuring that the vendor will take proper care of the data. Once data is recovered the original hard drive must be returned to the owner so that the owner can dispose of it per this UMBC policy for proper disposal of electronic media.

iv. Disposal of Damaged or Inoperable Hard Drives

The owner must first attempt to ***Purge*** the hard drive in accordance with the method described under sanitization types. If the hard drive can not be ***Purged***, the hard drive must be ***Destroyed*** in accordance with the method described above under sanitization types. Alternately, an owner may immediately ***Destroy*** a hard drive without first attempting to ***Purge*** the hard drive. The use of certified commercial disposal vendors may be excepted with prior approval by the office of the VPAF and campus legal counsel.

B. Disposal of Electronic Media Other Than Hard Drives

Prior to disposal or transfer, Electronic Media Other Than Hard Drives, must be ***Cleared, Purged*** or ***Destroyed*** in accordance with the methods described within this policy.

i. Transfer of Electronic Media Other Than Hard Drives

1. **IntraDepartmental:** *Transfer of electronic media (other than hard drives) within a department.* Before electronic media is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Since the electronic media is remaining within the department, the electronic media may instead be ***Cleared, if possible,*** prior to transfer. Special recovery tools must be used by an individual to access the data erased by this method; any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the *UMBC Acceptable Use Policy*

2. **InterDepartmental:** *Transfer of electronic media (other than hard drives) to another department.* Before electronic media is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. All electronic media should be ***Purged, if possible*** in a manner described above. If the electronic media can not be ***Purged*** it may not be transferred to an external department.

ii. Disposal of Electronic Media Other Than Hard Drives Outside of UMBC

All electronic media other than hard drives, containing sensitive or proprietary data, must be ***Purged*** or ***Destroyed*** before leaving UMBC. The use of certified commercial disposal vendors may be excepted with prior approval by the office of the VPAF and campus legal counsel.

VIII. VIOLATION OF THIS POLICY

If there is a reasonable basis to believe that the proper procedures as outlined in this policy have not been or are not being followed, a report must be filed with the Information Security Officer. If improperly sanitized electronic media is found, then the media should be reported to the appropriate departmental I.T. support personnel.

IX. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, including but not limited to, termination under the appropriate University disciplinary policy.

X. REFERENCE POLICIES & GUIDELINES

- **A.** National Institute of Standards and Technology Special Publication 800-88 Natl. Inst. Stand. Technol. Spec. Publ. 800-88, 41 pages (May, 2006) *Guidelines for Media Sanitization*
- **B.** X-1.00.01 UMBC Policy for Responsible Computing *September 6, 1996*
- **C.** X-1.00.07 UMBC's Definition of Non-Public Information *Draft Dated November 2006*

Policy Number: X-1.00.05 (formerly unnumbered)
Category: Miscellaneous - IT
Responsible Administrator: Michael Carlin
Responsible Office: Division of Information Technology
Originally Issued: *DRAFT Approved* August 7, 2007
Revised:
Amended:
Revised:
Revision Approved: