UMBC

AN HONORS UNIVERSITY IN MARYLAND

UMBC POLICY FOR RESPONSIBLE COMPUTING
UMBC Policy X-1.00.01

I. POLICY STATEMENT

This Policy sets forth the principles that govern appropriate use of computing and digital information resources. Such resources are the property of the State of Maryland, and users are bound by all pertinent University, State, and Federal policies and statutes. Access to UMBC computing resources is a privilege granted by the University. Computing policies, like other university policies, where ever possible are governed by the principle of academic freedom.

II. PURPOSE FOR POLICY

UMBC provides access to computing and information resources for students, staff, faculty, and certain other users in support of UMBC's mission of teaching, research, public service, and in support of the official duties of the University. When activating an account, a user implicitly affirms that: they will abide by the broadest interpretation of the following policies; failure to follow policies may result in loss of computing privileges; UMBC may monitor computer use to protect the system; and the university may terminate the account of anyone who has been determined to use his or her access for unlawful purposes or in contravention of this policy. Computer users shall:

1. Act responsibly so as to ensure the integrity and ethical use of computing and information resources.
2. Respect the rights of others, and not threaten, harass, intimidate, or commit theft or fraud.
3. Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.
4. Use University computing resources and user accounts only for appropriate University activities.
5. Acknowledge that system administrators may examine files, mail, and printer listings for the purpose of diagnosing and correcting problems with the system.
6. Acknowledge the right of the University to restrict or rescind computing privileges for cause.

III. APPLICABILITY AND IMPACT STATEMENT

This policy addresses the entire UMBC campus community.

IV. CONTACTS

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

Subject	Contact	Telephone	Email
Policy Clarification	DoIT	410-455-2585	jack@umbc.edu

V. UNIVERSITY POLICY

A. EXAMPLES OF ACTIVITIES SPECIFICALLY PROHIBITED

The following are some of the things that are prohibited activities; this list in not inclusive. No person may:

1. Intentionally corrupt, misuse, or steal software or any other computing resource.
2. Access information resources, data, equipment, or facilities in violation of any restriction on use.
3. Use University computing resources for personal or private financial gain without written authorization. Excepted from this provision is remuneration to faculty and staff for customary university related activities from: approved consulting; copy rights; patents; royalties; honoraria; reviews; etc.
4. Use another person's computer account.
5. Establish an independent computer system, except those specifically authorized for departmental use.
6. Knowingly, without written authorization, execute a program which may hamper normal computing activities at UMBC or elsewhere.

B. ACTION TO PRESERVE PUBLIC SAFETY OR INTEGRITY OF COMPUTING RESOURCES

If an University Computing Services (UCS) official reasonably believes that a user is engaged in activities which may pose an imminent threat to: 1) the health or safety of others; 2) the integrity of data; or 3) computing resources which may adversely affect system operations, the official may temporarily suspend user privileges for no more than two working days (excluding weekends and university holidays) before consulting an Administration official. In all other cases, the UCS official shall consult the Associate Vice President for Academic Affairs and follow existing University procedures, where applicable, prior to:

1.Investigating alleged improper or illegal use of data, programs, or UCS equipment or resources;
2.Accessing data and files pertinent to the investigation; or
3.Limiting user privileges until the matter is resolved. If appropriate, or required, findings from investigations may be reported to other University officials for review and action, or to State or Federal authorities.

C. INFORMING USER OF ACTIONS TAKEN

Unless such notification may impede an investigation, within one week University officials shall disclose in writing to an affected user that:

1. The user's account has been suspended, or that
2. The user is under investigation, and that
3. The user may submit evidence to those conducting the investigation, and the procedures that are applicable to the investigation.

D. ACKNOWLEDGMENT OF POLICY

By activating a computing account, a user implicitly agrees to abide by the above policy in its entirety.

:

VI. DEFINITIONS

Responsible Administrator	The Vice President or senior administrator charged with the responsibility for creating, implementing, updating and enforcing University Policies as required in his/her area of administrative authority.
Responsible Department or Office	At the direction of the Responsible Administrator, the Responsible Department or Office develops and administers policies and procedures and assures the accuracy of its subject matter, its issuance, and timely updating.

VII. APPROVAL AND PROCEDURES

A. Pre-approval is not applicable.

B. Approval is not applicable

C. Procedures: See note above regarding procedures. Note: Should any forms or procedures outside of the policy apply, the "link" to these documents is to be included here.

VIII. DOCUMENTATION: NA

IX. RESTRICTIONS AND EXCLUSIONS: *NONE*

X. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES: *NONE*

Administrator Use Only

Policy Number: 1.00.01
Policy Section: X-Information Technology
Responsible Administrator: VP-DoIT
Responsible Office: Division of Information Technology (DoIT)
Approved by President: 9/26/96
Originally Issued: 9/26/96
Revision Date(s): 1/14/2009 (Converted to PDF for Policy website.)