UMBC
AN HONORS UNIVERSITY IN MARYLAND

UMBC INFORMATION TECHNOLOGY SECURITY POLICY
UMBC Policy # X-1.00.02

I. POLICY STATEMENT

UMBC's Information Technology (IT) Security Policy is the basis for the university's IT security program. Information and IT systems are vital assets that enable UMBC to accomplish its mission and strategic priorities. UMBC's IT systems are centrally managed but the overall IT infrastructure is a distributed and shared environment. As the IT infrastructure grows and becomes more complex, increasing amounts of administrative or academic personal, proprietary, or institutional data is being stored, accessed, and manipulated electronically, increasing the risk of unauthorized access, disclosure, or modification. UMBC must, therefore, maintain an effective IT security program to mitigate the risks posed to its IT resources.

II. PURPOSE FOR POLICY

The purpose of this policy is to establish an IT security framework for ensuring that the university's IT resources are protected and managed securely. These resources include electronic data, information systems, computing platforms, and networks.

III. APPLICABILITY AND IMPACT STATEMENT

UMBC's IT security policy applies to all university information resources and impacts all users who access those resources. It especially pertains to university systems that support vital business functions and/or that maintain sensitive personal or institutional information.

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 Address
Policy Clarification	Vice President of IT	(410) 455-3208	jack@umbc.edu

V. UNIVERSITY POLICY

UMBC establishes and maintains a security program that enhances and protects the integrity, confidentiality, and availability of UMBC's IT resources and complies with applicable federal and state laws. This program encompasses the following elements:

- Risk assessments of IT resources;
- Access controls to computing environments and electronic data;
- Network security;
- Monitoring, incident response, and reporting;
- Business continuity and disaster recovery;
- Security awareness, education, and training;
- Data management, classification, and control; and
- Organizational responsibilities.

Each of these elements may be supplemented by additional policies, compliance guidelines, and best practices.

VI. DEFINITIONS

Information Technology Resources	• All university-owned computers, applications software, systems software, databases, and peripheral equipment; • The data communications infrastructure; • The voice communications infrastructure, and; • Classroom technologies; communication services and devices, including electronic mail, voice mail, modems, and multimedia equipment. Components thereof may be stand-alone or networked and may be single-user or multi-user systems.
Responsible Administrator	The Vice President for Information Technology is the senior administrator responsible for creating, implementing, updating, and enforcing UMBC's IT Security Program.
Responsible Department or Office	The Division of Information Technology develops and administers the policies, procedures, and technical measures (devices and processes) needed to implement and enforce UMBC's IT security policy and program.

VII. APPROVAL

A. The Data Management Council and the IT Steering Committee shall review and recommended approval of modifications to guidelines and procedures associated with this policy.

VIII. PROCEDURES

Applicable procedures, guidelines, and best practices supplementing each of the bulleted items in Section V. above are/will be posted on the DoIT web site.

IX. DOCUMENTATION: N/A

X. RESTRICTIONS AND EXCLUSIONS: None

XI. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES: Applicable procedures, guidelines and best practices supplementing each of the bulleted items in Section V. above are/will be posted on the DoIT web site.

Policy Number:	**UMBC X-1.00.02**
Policy Section:	**Section X: Information Technology**
Responsible Administrator:	**Vice President for Information Technology**
Responsible Office:	**Division of Information Technology**
Approved by President:	**Unknown; February 2009**
Originally Issued:	**March 2003**
Revision Date(s):	**1/14/2009**