UMBC INFORMATION TECHNOLOGY SECURITY POLICY
UMBC X-1.00.02

RATIONALE
Innovations in digital technologies have markedly increased the use of information technologies in all facets of university life. As such, information and information systems are increasing perceived as vital assets, enabling the accomplishment of the university's mission and strategic priorities.

While administrative systems are centrally managed at UMBC, the overall information technology infrastructure is a distributed and shared environment. At the same time, much more administrative and academic information is being stored, accessed, and manipulated electronically, increasing the risk of unauthorized disclosure or modification of personal, proprietary, or institutional data. UMBC must, therefore, maintain effective security programs to mitigate the risks posed to its information technology resources.

*PURPOSE:* The purpose of this policy is to establish a framework for ensuring that the university's information technology resources are managed securely. These resources include information, information systems, computing platforms, and networks.

*SCOPE:* This security policy applies to all university information resources and all users who access those resources. While the policy applies to all information resources, it especially pertains to university systems that support vital business functions and those that maintain sensitive personal or institutional information.

*GENERAL POLICY:* It is the policy of UMBC to establish and maintain a security program that enhances and protects the integrity, confidentiality, and availability of information resources and is in compliance with applicable laws. This program will encompass the following elements:

* Risk assessments of information technology resources;
* Access controls to computing environments and information;
* Network security;
* Monitoring, incident response and reporting;
* Backup and recovery;
* Security awareness, education, and training; and
* Organizational responsibilities.

Equally important, the university recognizes its responsibility to promote an open computing environment that allows access to university computing resources to individuals for authorized purposes. The university has separate policies and guidelines that address the acceptable use of information technology resources; sanctions for the misuse of abuse of university information resources; privacy of
electronic information; use of electronic mail; disaster recovery; and others. In addition, the Chief Information Officer or designate has the authority to logically isolate a system from accessing university IT services or the network if that system puts other resources at risk.

DEFINITIONS: Information Technology Resources- Information Technology Resources includes all university-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; classroom technologies; communication services and devices, including electronic mail, voice mail, modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.

RELATED POLICY REFERENCES:

X-1.00.01 UMBC Policy for Responsible Computing

IT-02 UMBC Guidelines for Securing University IT Resources

IT-03 UMBC Guidelines for Using Electronic Mail

X-1.00.06 UMBC Policy on Web Site Privacy

*RESPONSIBLE ORGANIZATION:* UMBC Office of Information Technology

oit@umbc.edu

http://www.umbc.edu/oit

Approved: Unknown

Last Revised: January 14, 2009 (Converted to PDF for Policy Site)