

University of Maryland Baltimore (UMB) Information Technology Security Policy

Effective Date: 04/14/03

Purpose

The purpose of this policy is to establish a framework for ensuring that UMB's information technology resources are managed in a secure fashion. It is also intended to address issues of confidentiality, data integrity, availability, accountability and responsibility.

Computer information systems are increasingly vulnerable to hacking and break-ins. Intruders find that the Internet provides access to computer systems around the world. It is UMB's responsibility to protect and maintain the information it is charged with managing. Personnel and IT administrators are obliged to prevent trespassers from corrupting or misusing UMB software or hardware. Listed below are security practices that are to be followed where technically feasible.

Definitions

"Affiliate": an organization located at the UMB campus which has IT Resources connected to UMB IT Resources, or which has IT Resources used by Personnel; also an organization located elsewhere which provides IT Resources used by Personnel in the course of UMB employment or educational activities.

"Affiliate IT Resources": IT Resources that are owned by, or under the direction or control of, an Affiliate of UMB.

"Critical enterprise systems": centrally managed systems and services that support critical business functions and that maintain confidential, sensitive, private, personal or institutional information, including the majority of systems and services that are managed centrally. Examples are the campus network and connectivity to the Internet, administrative systems such as human resources, payroll, finance, student records, and registration. Critical enterprise systems are designated by the UMB Chief Information Officer.

"Information technology resources or IT Resources": information technology resources including, but not limited to, computerized information, computing facilities, systems and devices, network systems, resources and devices, software, e-mail systems, and web pages.

"IT Administrator": the administrator or academic officer of a UMB unit or school who, as determined by the applicable vice president or dean, is responsible for management and oversight of the UMB IT Resources and Affiliate IT Resources located in, or used by Personnel of, that unit or school.

"Personnel": all students, faculty, staff, visitors, and guests who use UMB IT Resources, on-campus or off-campus, or who use Affiliate IT Resources in the course of UMB employment or educational

activities; also, employees of Affiliates who use UMB IT Resources to fulfill employment responsibilities.

"UMB": University of Maryland Baltimore.

"UMB IT Resources": IT Resources that are owned by, or under the direction or control of, UMB, as well as IT Resources for which UMB otherwise is responsible.

Scope

This policy applies to all University information technology resources and Personnel who access those resources. It pertains especially to those resources that support critical enterprise systems.

General Policy

It is the policy of UMB to maintain an IT security program that protects the integrity, confidentiality, and availability of information resources, as well as addresses compliance with all applicable laws and regulations. The program will encompass the following elements:

1. Risk assessments of information technology resources
2. Access controls to computing environments and information
3. Network security, including firewalls, virtual private networks, etc.
4. Monitoring, incident response and reporting
5. Disposal and reuse of storage media for critical enterprise systems
6. Backup and recovery of critical enterprise systems
7. Security awareness, training and education
8. Clearly defined organizational responsibilities for security

UMB recognizes the responsibility for promoting an open computing environment. Access to critical enterprise systems will be provided for individuals with appropriate authorization. UMB has separate standards and policies that address the various topics within its security program. These standards and policies are listed under the "Related Policies/Standards" section of this document.

Related Policies/Standards

Information Technology Acceptable Use Policy
Information Technology Privacy Policy
Policy on Privacy of Protected Health Information (HIPAA)

Server Security Standard
Workstation Security Standard
Wireless Security Standard
Network Standards

APPROVED BY THE PRESIDENT:

David J. Ramsay, D.M., D.Phil.

Date