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. The IT Security Policy is designed to maintain compliance with the University System of Maryland (USM) IT Security Standards, and be functionally compatible with the State of Maryland’s IT Security Policy. The elements of the UMBC IT security program listed below must be in place in order to meet the aforementioned standards. As IT and cybersecurity threats evolve over time, so will aspects of the IT security program. In order to fulfill these requirements the Division of Information Technology (DoIT) is the lead organization in developing and implementing UMBC’s IT security program, including requirements for security awareness training and compliance. UMBC DoIT is the operational arm of implementing the USM Board of Regents’ IT Security Standards, and will work through UMBC’s shared governance process on creating IT guidelines and practices to fulfill these requirements. Security at UMBC is everyone’s responsibility so that UMBC community members can successfully learn and work as they interact with University systems.

Information and IT systems, including networks, devices, software, and data, are vital assets that enable UMBC to accomplish its mission and strategic priorities. 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, whether inadvertent or malicious. UMBC must therefore maintain an effective IT security program by using a risk-management based approach and continuously mitigating 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 physically and logically protected and managed securely. These resources include but are not limited to electronic data, information systems, computing platforms, and networks.

III. APPLICABILITY AND IMPACT STATEMENT

UMBC's IT Security Policy applies to all University IT Resources, including the use of personal or contractor-owned devices for processing institutional information, and impacts all users who access those resources.

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	Division of Information Technology (DoIT)	410-455-3208	itpolicy@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 based on the National Institute of Standards and Technology (NIST) Risk Management Framework;
- Acceptable Use Policy;
- Incident Response Plan;
- Access controls to computing environments and electronic data;
- Change Management procedures;
- Systems Development Lifecycle plans;
- 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 and compliance guidelines developed through UMBC's shared governance process, and vetted by the IT Steering Committee, of which the UMBC Chief Information Security Officer (CISO) is a member.

VI. DEFINITIONS

UMBC Community	Any student, alumnus, faculty member, staff member, research associate, contractor, anyone who is granted access, or visitor who uses UMBC facilities and resources.
Information Technology Resources (IT Resources)	• All University-owned computers, classroom technologies and peripheral equipment; licensed or developed applications software, systems software, or databases; and third party and cloud services; ● Anything using or connecting to UMBC's communications infrastructure. • Institutional computing resources, including email, messaging, documents and digital information assets.
Responsible Administrator	The UMBC Chief Information Officer (CIO) is the senior administrator responsible for creating, implementing, updating, and enforcing University Policies as required in their area of administrative authority.
Responsible Department or Office	At the direction of the CIO, the DoIT, in conjunction with other offices as appropriate, develops and administers the policies, procedures, and assures the accuracy of its subject matter, its issuance, and timely updating.

VII. APPROVALS AND PROCEDURES

1. The IT Steering Committee shall review and recommend approval of modifications to guidelines and procedures associated with this policy.
2. DoIT will work with university leadership and shared governance with communicating applicable procedures, guidelines and best practices.

VIII. DOCUMENTATION: N/A

IX. RESTRICTIONS AND EXCLUSIONS: None

X. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES

USM IT Security Standards
https://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

USM Policy X-1.00 Policy on USM Institutional Information Technology Policies
(Including Functional Compatibility with The State Information Technology Plan)

X-1.00.01 - UMBC Acceptable Use Policy

X-1.00.03 - UMBC Policy on Password-Based Credential Management

X.1.00.04 - UMBC Policy on Firewalls

X.1.00.05 - UMBC Policy on Electronic Media Disposal

X.1.00.06 - UMBC Policy on Web Site Privacy Statement

X.1.00.08 - UMBC Policy on Cell Phone Usage

X.1.00.09 - UMBC Policy on the Classification and Protection of Confidential Information

---

Administrator Use Only

Policy Number: UMBC X-1.00.02
Policy Section: Section X: Information Technology
Responsible Administrator: Chief Information Officer - DoIT
Responsible Office: Division of Information Technology
Approved by President: 2/2009, 4/15/25
Originally Issued: 3/2003
Revision Date(s): 4/15/25