UMBC Policy on Credential Management, Authentication, and Authorization
UMBC Policy # X-1.00.03

I. POLICY STATEMENT

In order to provide for secure authentication and appropriate access control to UMBC systems, and to comply with the University System of Maryland's (USM) IT Security Standards, UMBC is implementing the following policy on the issuance of credentials to individuals, authentication requirements for using those credentials to access UMBC services, and the appropriate authorization for those credentials to access services.

II. PURPOSE FOR POLICY

In order to provide secure authentication to access UMBC systems, and to comply with the University System of Maryland's IT Security Standards, UMBC is implementing the following policy for all users of its systems. In order to comply with the USM's IT Security Standards, UMBC has established its IT Security Policy, which places the Division of Information Technology (DoIT) in charge of implementing security requirements for the University. As part of that responsibility, DoIT has developed guidance for the issuance, management, and usage of UMBC assigned credentials that provide access to UMBC IT services, referred to as credential management.

DoIT is responsible for setting the appropriate requirements that must be met by users when using these credentials in order to satisfy UMBC's IT security requirements under USM 5.0 guidance. As part of this responsibility, DoIT will enforce, through technology or policy, the authentication standards and practices deemed necessary for appropriately securing UMBC resources. DoIT will also be responsible for providing guidance and training resources for the UMBC community regarding safeguarding credentials, defining appropriate authentication requirements based on risk, and working with Data Stewards to establish the appropriate authorization used for access control to IT services.

III. APPLICABILITY AND IMPACT STATEMENT

This policy addresses all UMBC students, faculty, staff, and users of UMBC accounts.

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

Each individual is issued one primary credential that works for all services and will evolve with you as your roles at UMBC change. Whether accepting matriculation for students, employment for employees, or a visitor being sponsored access, all individuals are required to select a credential, which we call a username, create a strong authentication token, such as a password, and acknowledge they are bound to our Acceptable Use Policy. Credentials are never reassigned or reused and we collaborate with Campus Card services to validate your identity with an outside ID. We require individuals to have a secondary email account somewhere other than UMBC to receive a UMBC credential in case they get locked out of their UMBC account and we need to reach them.

UMBC utilizes a risk-based approach towards protecting its IT Resources and systems. First, all IT systems are reviewed for risk based on the UMBC Policy on Classification and Protection of Confidential Information. Second, UMBC assigns an internal level of assurance to each user based on that individual's role and authorization to IT systems and services they have access to. Combining those two factors determines the level of assurance for a person, which in turn dictates the authentication requirements.

DoIT works closely with campus Data Stewards, Campus Card, Library, Registrar, Procurement, and Human Resources to develop our identity management system (IDMS) to manage and coordinate credentials and associated internal account identifiers. Many systems have specific requirements for internal account identifiers. The combination of the myUMBC single-signon and the IDMS abstracts the complexity of all these systems so users only need one set of credentials.

To ensure all on-campus and third-party IT services have the same level of authentication security, we require all IT systems and services, unless there is a waiver approved by DoIT, to use the myUMBC single sign-on. This requirement has been approved by our Campus Systems Executive Committee (CSEC) as part of our UMBC Procurement of Software-as-a-Service contracts. Since our single sign-on fully supports the InCommon Federation standards for authentication and authorization, researchers may use their UMBC credentials for NIH or NSF services.

For all credentials assigned to individuals, we use a risk-based approach to authentication and authorization. For authentication, UMBC's authentication guidelines are functionally compatible with the best practices established by the National Institute for Standards and Technology (NIST). In the case of passwords, we follow NIST Special Publication 800-63-3B Section 5.1.1.2 Memorized Secret Authenticators. NIST 800-63 puts forth a science-based approach for password construction and aging rules allowing an institution to build a policy that best fits its business needs, and sets standards for credential revocation, change, and maintenance. Please see UMBC's password guidelines to learn more about the procedures for users of its enterprise authentication system. For authorization, please refer to the section on responsibilities of Data Stewards in the UMBC Policy on Classification and Protection of Confidential Information. Data Stewards are required to periodically review authorization levels.

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 electronic communications such as email and messaging, documents and other digital information assets.
Multi-factor Authentication	A multi-step account login process that requires users to enter two or more verification factors, rather than a single authentication mechanism.
Password	A string of characters used for authenticating a user on a computer system.
Responsible Administrator	The UMBC Chief Information Officer (CIO) is the senior administrator charged with the responsibility 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 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 policy above regarding procedures.

VIII. DOCUMENTATION: N/A

IX. RESTRICTIONS AND EXCLUSIONS: None

X. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES:

X.1.00.01 - UMBC Acceptable Use Policy

X.1.00.02 - UMBC Information Technology Security Policy

USM IT Security Standards 5.0

NIST 800-63-3: Digital Identity Guidelines

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

Administrator Use Only

Policy Number: UMBC X-1.00.03
Policy Section: Section X: Information Technology
Responsible Administrator: Chief Information Officer - DoIT
Responsible Office: Division of Information Technology
Approved by President: 1/2007, 4/15/2025
Originally Issued: 1/2007
Revision Date(s): 4/15/2025