UMBC INTERIM POLICY ON
THE PROTECTION OF CONFIDENTIAL INFORMATION
UMBC Policy # X-1.00.09

I. POLICY STATEMENT

Data and information are important assets of the University and must be protected from loss of integrity, confidentiality, or availability in compliance with University policy, state and federal law and regulations.

The purpose of this document is to provide guidance in complying with Section III, Confidential Information Standard, of the USM IT Security Standards. This section states that USM institutions are required to establish an institutional policy for the protection of Confidential Information.

II. PURPOSE FOR POLICY

This policy is intended to provide UMBC employees (faculty and staff) and 3rd party contractors with a basic understanding of their responsibilities to protect and safeguard the Confidential Information to which they have access as a result of their employment.

III. APPLICABILITY AND IMPACT STATEMENT

This policy applies to all UMBC Employees and 3rd Party Contractors.

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 office:

Subject	Contact	Telephone	Email
Policy Clarification	Mark Cather (CISO)	410-455-3783	mark.cather@umbc.edu

V. UNIVERSITY POLICY

To safeguard Confidential Information, the general rules below must be followed:

A. All employees with job duties that require accessing or processing Confidential Information are required to safeguard such information at all times. Employees may only use or disclose Confidential Information as expressly authorized or specifically required in the course of performing their specific job duties.

B. Employees are prohibited from sharing their user credentials or permitting another person to access Confidential Information in data bases and/or systems.

C. Employees who have access to Confidential Information are expected to know and understand associated security requirements, and to take measures to protect the information, regardless of the location of the data, e.g., cloud solutions, local personal computers, server file shares, physical storage environments (offices, filing cabinets, drawers), and magnetic and optical storage media (hard drives, diskettes, tapes, CDs, flash drives). Computer display screens should be positioned so that only authorized users can view Confidential Information, and Confidential Information should be discarded in a secure way that will preserve confidentiality (e.g., in a shred box, not in a trash can or recycling bin).

D. Paper records containing Confidential Information must be protected at all times and stored in physically secure locations when not in use.

E. Electronic records containing Confidential Information must be stored on secure servers.

F. Confidential Information must not be stored on any mobile devices, including notebook computers, smart phones, external hard drives, USB thumb drives; without written administrative approval.

G. When it is necessary to transport records containing Confidential Information, employees must safeguard the information and never leave it unattended.

H. When there is a legitimate need to provide records containing Confidential Information to a third party, employees must ensure that the receiving party will provide protection to the information that is equal to or greater than the protection required by UMBC and University System of Maryland information security requirements. Employees must ensure that Confidential Information is provided to a third party in an approved secure manner. Employees must also ensure that the third party will properly dispose of UMBC Confidential Data and notify UMBC if any UMBC Confidential Information is breached through any systems under the control of the third party.

I. Employee misuse of Confidential Information and/or the systems in which the information is stored is a serious breach of job responsibilities and will result in disciplinary action up to and including termination of employment. As appropriate, criminal charges may also be filed for the misuse of Confidential Information or UMBC computing systems.

J. Employees must report any suspected violation of this policy or breach of Confidential Information to the UMBC Chief Information Security Officer immediately.

K. Employees must abide by all applicable local, state, and federal laws and regulations with regard to information protection, information breaches, and privacy.

VI. DEFINITIONS

Confidential Information	Under Maryland Code, State Government Article, §10-1301 (SB 676 - 2012), personal information is defined as: An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: • a social security number; • a driver's license number, state identification card number, or other individual identification number issued by a unit; • a passport number or other identification number issued by the united states government; • an individual taxpayer identification number; or • a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account. Employment and Personnel Records Records of Workplace or Academic Accommodation Education Records, as defined and when protected by 20 U.S.C. § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades In addition, any Protected Health Information (PHI), as the term is defined in 45 Code of Federal Regulations 160.103 (HIPAA)
Responsible Administrator	The Vice President or senior administrator charged with the responsibility for creating, implementing, updating and enforcing University Policies as required in his/her area of administrative authority.
Responsible Department or Office	At the direction of the Responsible Administrator, the Responsible Department or Office 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 section above.

VIII. DOCUMENTATION: None

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 #III-6.30 Policy on Confidentiality and Disclosure of Student Records
https://www.usmd.edu/regents/bylaws/SectionIII/III630.html

Administrator Use Only

Policy Number: X-1.00.09
Policy Section: Information Technology
Responsible Administrator: Mark Cather-Chief Information Security Officer
Responsible Office: DoIT
Approved by President: 6/12/2020
Originally Issued: 6/12/2020-Interim
Revision Date(s): _____ (date)