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

## I. POLICY STATEMENT

Data and information are important assets of UMBC and must be protected from loss of integrity, confidentiality, or availability in compliance with University policy, state and federal law and regulations. Members of the UMBC Community are responsible for properly using and, when appropriate, protecting Confidential Information that has been collected, produced, or maintained by UMBC in connection with its educational and research mission and/or operation as a public university. Confidential Information must be assigned a level of protection that is commensurate with the type of information and the purpose for which it was collected, obtained, or produced.

This policy is intended to provide guidance in complying with the University System of Maryland (USM) IT Security Standards. Assigning the appropriate level of protection to Confidential Information is called data classification. Some UMBC Data and Information is classified as public information, per the Maryland Public Information Act, and can be disclosed upon consideration of statutory denials. However, some UMBC Data and Information is classified as confidential because it is personally identifiable, UMBC proprietary institutional information, sensitive research data, or information that is controlled by laws or regulations. UMBC Data Stewards must identify and appropriately classify Confidential Information so it is disclosed, stored and protected appropriately.

Members of the UMBC Community must know the difference between public information and Confidential Information and how to classify and protect Confidential Information.

## II. PURPOSE FOR POLICY

The purpose of this policy is to protect Confidential Information within the UMBC Community from unauthorized access, use, or disclosure. Every employee is obligated to protect confidential information and should be aware of the four data classification levels used to identify and secure Confidential Information. The goal is to assure that every member of our community and 3rd party contractors who have access to Confidential Information should be able to appropriately classify that information and follow appropriate security precautions to protect the information.

## III. APPLICABILITY AND IMPACT STATEMENT

This policy applies to individuals accessing and safeguarding UMBC Data and Information. All members of the UMBC Community who have access to UMBC Data and Information must understand these definitions and evaluate their actions consistent with UMBC policies for safeguarding the privacy of information. All UMBC Data Stewards, as well as individuals accessing UMBC Data and Information, beyond that which is considered self-service data on themselves, should read this policy.

## 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 | Division of Information Technology (DoIT) | 410-455-3208 | itpolicy@umbc.edu |

## V. UNIVERSITY POLICY

### A. DATA CLASSIFICATION

The UMBC Data Stewards must identify the data classification level for any data and information they are maintaining based upon the data classification. This classification level will range from Level 0 to Level 3. As data classification levels increase from 0 to 3, more secure technical and procedural security requirements must be implemented. For research data, UMBC follows the data classification scheme below unless the research sponsor has a specific data use agreement that proscribes specific data protection requirements.

Please see the table below for introductory guidance, but it is recommended that Data Stewards consult with related guidelines, the UMBC Chief Information Security Officer (CISO), privacy officer, and Office of General Counsel if any questions arise. The UMBC Data Use Guidelines provide information on the appropriate use and level of protection required for all levels of Confidential Information.

When there is a legitimate need to provide records containing Confidential Information to a third party, Data Stewards must ensure that the receiving party, such as third party Software-as-a-Service (SaaS) application vendors, will provide protection to the Confidential Information that is equal to or greater than the protection required by UMBC and USM information security requirements. Data Stewards must ensure that Confidential Information is provided to a third party using the security requirements determined to be the highest among the sharing institutions involved and approved by the CISO. Data Stewards must also ensure that the third party will properly dispose of UMBC Confidential Data and notify UMBC if any UMBC Confidential Information is exposed through any systems under the control of the third party.

Data Stewards must report any suspected violation of this policy or exposure of Confidential Information to the UMBC CISO immediately. The CISO will then report any incidents involving the compromise of personal information (as defined under State Government Article 10-301, see Section III) or confidential information (as defined below) to the USM at security@usmd.edu.

| **Information Classification** | **Definition** | **Examples** |
|---|---|---|
| Level 3 | Highest risk data, systems and applications or services that have externally mandated IT compliance requirements such as those containing information covered by HIPAA or PCI.  Failure to comply with these externally mandated IT Security requirements would result in serious financial, legal and/or reputational harm to individuals and/or the University. | ● Payment Card Industry Data Security Standard (PCI-DSS) Data<br>● Controlled Unclassified Information (CUI)<br>● Export-Controlled Information<br>● Health Insurance Portability and Accountability Act (HIPAA) data |
| Level 2 | Critical data, systems, applications or services related to or supporting the commitment or management of UMBC financials, student data, research, and those systems containing sensitive information (i.e. name, SSN or other combination or personal identifiers) which if compromised could be used to commit identity theft. | ● Personal information, as defined under the Maryland Code, State Government Article, §10-1301 - §10-1308<br>● Identifiable data elements that contain sensitive health information that are not otherwise subject to HIPAA |
| Level 1 | Data intended for internal University use. Applications or services that support academic instruction, research data or general communications that do not contain sensitive information. | ● Non-PII student records<br>● Employment and Personnel records |
| Level 0 | Non-critical data (i.e., public directory information). Data explicitly or implicitly approved for distribution to the public where there is little institutional risk associated with this system due to security. | ● Data made freely available by public sources<br>● Published data<br>● Summarized |

| | | |
|---|---|---|
| | | Educational data<br>● Initial and intermediate Research Data |

## VI. DEFINITIONS

| | |
|---|---|
| **Confidential Information as Defined by USM** | Personal information, as defined under the Maryland Code, State Government Article, §10-1301 - §10-1308, includes:<br>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:<br>● a social security number;<br>● a driver's license number, state identification card number, or other individual identification number issued by a unit, as defined in COMAR;<br>● a passport number or other identification number issued by the United States government;<br>● an individual taxpayer identification number; or<br>● 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. |
| **Additional Confidential Information as Defined by UMBC** | ● Employment and Personnel Records.<br>● Records of Workplace or Academic Accommodation. |
| **Educational Records** | Educational 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. |
| **Protected Health Information** | Any Protected Health Information (PHI), as the term is defined in 45 Code of Federal Regulations 160.103 (HIPAA). |
| **UMBC Data and Information** | Data or information, in physical or electronic format, that is or has been collected, produced, controlled, or maintained by UMBC in connection with its educational and research mission and/or operation as a public university, including both public information and Confidential Information. |
| **Data Stewards** | The persons or offices responsible for granting access and administrative control over specific UMBC Data and Information while protecting the data as defined by UMBC's Security Policy, IT Security Policy or Data |

| | |
|---|---|
| | Use Guidelines. This also pertains to Principal Investigators responsible for research data. |
| **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. |

## VI. APPROVAL AND PROCEDURES

A. Pre-approval is not applicable.
B. Approval is not applicable.
C. Procedures: See policy section above.

## VIII. DOCUMENTATION: N/A

## IX. RESTRICTIONS AND EXCLUSIONS: None

## X. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES:

UMBC Data Use Guidelines

UMBC X-1.00.05 - UMBC Policy on Electronic Media Disposal

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:** Section X: Information Technology
**Responsible Administrator:** Chief Information Officer – DoIT
**Office:** Division of Information Technology
**Approved by President:** 6/12/2020, 4/15/2025
**Originally Issued:** 6/12/2020
**Revision Date(s):** 4/15/2025