

**UMBC POLICY ON DEFINITION OF NON PUBLIC, PERSONALLY IDENTIFIABLE,  
AND UMBC PROPRIETARY INSTITUTIONAL INFORMATION  
UMBC#X-1.00.07**

**I. POLICY STATEMENT**

Members of the UMBC community are responsible for properly using and, when appropriate, protecting information, particularly **non-public information (NPI)**, **personally identifiable information (PII)**, and **UMBC proprietary institutional information (UPII)**, that has been collected, produced or maintained by UMBC in connection with its mission and operation as a public research university. The appropriate use and level of protection must be commensurate with the type of information and the purpose for which it was collected or produced. Most information under UMBC's control is public information, in physical and/or electronic format, and can be shared without constraint. However, some information is **non-public, personally identifiable**, or **UMBC proprietary institutional** information, in physical and/or electronic format, and must be protected and shared or used only on a need-to-know basis with the permission of the information's owner or custodian. Members of the UMBC community must know the difference between public and **non-public, personally identifiable**, and **UMBC proprietary institutional** information, and how to protect this information, whether it is about them, other members of the UMBC community, or proprietary UMBC information.

**II. PURPOSE FOR POLICY**

**Non-Public Information, Personally Identifiable Information and UMBC Proprietary Institutional Information** is being defined so every member of the UMBC community is able to recognize information that is or might be **sensitive**, so they can use and protect the information appropriately without jeopardizing their own privacy rights, other's privacy rights, or UMBC's institutional rights or obligations.

**III. ENTITIES AFFECTED BY THIS POLICY AND IMPACT STATEMENT**

This definition applies **sensitive** information being defined as, **Non-Public Information, Personally Identifiable Information and UMBC Proprietary Institutional Information**, in physical or electronic format, obtained by or from UMBC staff, faculty, students, contractors or visitors using UMBC facilities, services or IT systems. All members of the UMBC community who have access to, or come in contact with, **sensitive information** must understand these definitions and evaluate their actions consistent with UMBC policies for safeguarding the information.

**IV. WHO SHOULD READ THIS POLICY**

- A. Vice Presidents, Deans, Directors, and Department Heads
- B. Department administrators and business office staff
- C. Campus Senates, Steering Committee, and Standing Committees
- D. Individuals that have access to Sensitive information as defined in this policy

**V. 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:

<b>Subject</b>	<b>Contact</b>	<b>Telephone</b>	<b>Email</b>
Policy Clarification	Division of Information Technology		

**VI. DEFINITIONS**

<b>UMBC Community</b>	Any student, alumnae, faculty member, staff member, contractor or visitor who uses UMBC facilities and resources.
<b>Data Owner/Custodian</b>	The person responsible for, or the person with administrative control over, granting access to specific UMBC information while protecting the data as defined by the organization's Security Policy, IT Policy or Data Policy. Typically this is a senior level administrator on the campus (e.g. VP, Provost, etc.).
<b>Sensitive Information</b>	Information determined to be confidential because of laws, regulations, UMBC policy, or by agreement, whether the information is in physical or electronic format. UMBC places sensitive information into three categories, <b>Non-Public Information, Personally Identifiable Information</b> and <b>UMBC Proprietary Institutional Information</b> .
<b>Responsible Administrator</b>	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.
<b>Responsible Department or Office</b>	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.
<b>NPI</b>	Non-Public Information
<b>PII</b>	Personally Identifiable Information
<b>UPII</b>	UMBC Proprietary Institutional Information

## VII. UNIVERSITY POLICY

### UMBC DEFINITION OF NON-PUBLIC, PERSONALLY IDENTIFIABLE and UMBC PROPRIETARY INSTITUTIONAL INFORMATION:

UMBC considers information to be **Sensitive** if it is, or has been, determined to be confidential because of laws, regulations, UMBC policy, or by agreement, whether the information is in physical or electronic format. There are three categories of **sensitive information**:

- **Non-Public Information** about any member of the UMBC community, including, but not limited to:
  - Social Security Number
  - Banking and Credit Card Numbers
  - Medical Records, Including Psychological/Counseling Records
  
- **Personally Identifiable Information** about any member of the UMBC community, including, but not limited to:
  - Drivers License Number
  - Date and Place of Birth
  - Names of Relatives, Including Mother's Maiden Name
  - Financial Information
  - Academic Records of Matriculated Students
  - Disciplinary Records
  - Personnel Records
  - Educational Records (as defined within FERPA, see below)
  
- **UMBC Proprietary Institutional Information**, including, but not limited to:
  - Alumnae and Donor Records
  - Payroll Records
  - Copyrighted Information
  - Intellectual Property Including Unpublished Research, Unfunded Sponsored Project Proposals, and Patent Applications
  - Administrative Correspondence Containing Personally Identifiable Information or Otherwise Marked Confidential Due to its Content

**Sensitive information** of any type must always be protected and never disclosed without the consent of the owner or custodian, unless otherwise allowed by law. **Sensitive information** that is **Non-Public Information, Personally Identifiable Information** or **UMBC Proprietary Institutional Information**, must be subject to high standards of protection. All members of the UMBC community who have access to, or come in contact with, **sensitive information** must understand these definitions and evaluate their actions consistent with UMBC policies for

safeguarding the information. In the case of an unauthorized public disclosure of **Non-Public Information, Personally Identifiable Information** or **UMBC Proprietary Institutional Information**, the data **owner** or **custodian** ***must*** be promptly notified so as to determine the appropriate response and remediation.

**LEGAL REFERENCES:**

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Modernization Act of 1999 (also know as the Gramm-Leach-Bliley Act)
- Technology, Education, and Copyright Harmonization Act (TEACH Act)
- University System of Maryland Board of Regents Directives
- Maryland State Laws and Regulations

**RELATED POLICY REFERENCES:**

- X-1.00.01 UMBC Policy for Responsible Computing
- IT-02 UMBC Guidelines for Securing University IT Resources
- IT-03 UMBC Guidelines for Using Electronic Mail
- UMBC Disclosure of Student Records Procedure

**Policy Number: X-1.00.07 (formerly unnumbered)**

**Category: Miscellaneous - IT**

**Responsible Administrator: Michael Carlin**

**Responsible Office: Division of Information Technology**

**Originally Issued: *DRAFT Approved 10/17/2008***

**Revision Date(s):**