UMBC
AN HONORS UNIVERSITY IN MARYLAND

UMBC POLICY ON THE DEFINITION AND CLASSIFICATION OF SENSITIVE INFORMATION
UMBC Policy # X-1.00.07

I. POLICY STATEMENT

Members of the UMBC community are responsible for properly using and, when appropriate, protecting sensitive information that has been collected, produced or maintained by UMBC in connection with its research mission and/or operation as a public university. Sensitive 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.

Assigning the appropriate level of protection to sensitive information is called data classification. Much of the information under UMBC's control is classified as public information, in physical and/or electronic format, and can be shared without constraint. However, some information is classified as non-public because it is personally identifiable, UMBC proprietary institutional information, sensitive research data, or information that is controlled by laws or regulations. Whether in physical and/or electronic format, data owners and custodians must identify and appropriately classify sensitive information so it is protected appropriately.

Members of the UMBC community must know the difference between public information and sensitive information and how to classify and protect sensitive information.

II. PURPOSE FOR POLICY

The purpose of this policy is to protect sensitive information within the UMBC community from unauthorized access or disclosure. Every member of the community is obligated to protect sensitive information and should be aware of the four data classification levels used to identify and secure sensitive information. The goal is to assure that every member of our community can readily define sensitive information**,** such as SSN, or financial numbers in conjunction with a person's name, so they can appropriately classify the information, follow appropriate security precautions to protect the information, and not jeopardize the privacy rights of others or UMBC's institutional rights or obligations.

III. APPLICABILITY AND IMPACT STATEMENT

This definition applies to individuals accessing 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 information must understand these definitions and evaluate their actions consistent with UMBC policies for safeguarding the privacy of information. All

individuals that are data owners or custodians, as well as individuals accessing data, 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 offices:

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

V. UNIVERSITY POLICY

The data custodian or owner must define the data classification level for any records they are maintaining in electronic or physical form based upon the data sensitivity. This classification level will range from Level 0 (public) to Level 3 (access regulated by law or contract). 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. The data owner or custodian is responsible for informing DoIT of any data classified above level 0 so that the appropriate protections can be established.

- **Level 3**. Information specifically designated as sensitive by laws, regulations, or contracts; such as financial and health records or research contracts;
- **Level 2**. Personally identifiable information (e.g. SSN combined with number holder's name) protected by Federal or state laws, or data requirements from research sponsors.
- **Level 1**. UMBC proprietary institutional information; such as educational records protected FERPA or research contracts.
- **Level 0**. Public Information not classified as level 1-3.

The UMBC Data Use Guidelines provide information on the appropriate use and level of protection required for all levels of sensitive information.

LEGAL REFERENCES:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- University System of Maryland Board of Regents Directives
- Maryland State Laws and Regulations
- International Traffic in Arms Regulations (ITAR)

VI. DEFINITIONS

UMBC Community -Any student, alumnae, faculty member, staff member, research associate, contractor or visitor who uses UMBC facilities and resources.
Data Owner/Custodian -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. This also pertains to principal investigators responsible for research data.
Principal Investigator-The person responsible for the grant or sponsored contract as defined by the Office of Sponsored Programs.
Data Classification-This is a classification level of between 0 and 3, levels 2 and 3 deal with sensitive information that must be protected, with level 3 being a higher classification level.
Sensitive Information- Information that must be protected from unauthorized access or disclosure because of laws, regulations, UMBC policy, or by agreement, whether the information is in physical or electronic format.
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:

The UMBC Data Use Guidelines provide information on the appropriate use and level of protection required for all levels of sensitive information.

VIII. DOCUMENTATION: NA

IX. RESTRICTIONS AND EXCLUSIONS: None

X. RELATED ADMINISTRATIVE POLICIES AND PROCEDURES

- 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
- UMBC Security Risk Assessment
- UMBC Data Use Guidelines

Policy Number: X-1.00.07 (formerly unnumbered)
Category: Miscellaneous - IT
Responsible Administrator: Mark Cather
Responsible Office: Division of Information Technology
Originally Issued: DRAFT Approved 10/17/2008
Revision Date(s): Discussion draft 1/09/2013
5-17-2013 Modifications to draft based on feedback from IT Steering Committee
2-12-2014 Modifications to draft based on Maryland SB 676 (wlf)
of