University of Baltimore

III-3.3 Policy on Data Classification

Approved by President Schmoke on 1/10/2019

I. Purpose

As per the Institutional Data Management Policy, *the University of Baltimore's Institutional Data, by definition, practice and intent, are University assets. Institutional Data are owned by the University and not by individual persons, units, or departments of the University. Institutional Data will be safeguarded and protected. As University assets, Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction and/or inappropriate disclosure in accordance with established institutional policies and practices and federal and state laws. Data will be shared based on institutional policies. Institutional Data will be made accessible to all authorized users and systems, as defined in institutional policies.*

Members of the University Community are responsible for properly using and, when appropriate, protecting Institutional Data that has been collected, produced or maintained by the University. Based on Data Classification, non-public 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. Whether in physical and/or electronic format, data stewards and custodians must identify and properly classify sensitive information so it is protected appropriately. Members of the University Community must know the difference between public information and sensitive information and how to classify and protect non-public information.

This policy defines the guiding principles for the classification of Institutional Data and provides guidance to the University Community in complying with University policies and guidelines, University System of Maryland guidelines, as well as State and Federal laws and regulations when accessing, processing and/or storing such data.

II. Definitions

As per the Institutional Data Management Policy, the definition of "Institutional Data" is as follows:

A data element qualifies as Institutional Data if it is:

- Generated or collected in the course of or in furtherance of the business of the University;
- Exists in digital form, capable of being electronically stored or transmitted; and
- Resides or resided at any time in the past on any University-owned computer, server, or storage medium.
- Paper records that do not meet these criteria are not subject to this policy, although they may be subject to other, similar policies of the University.

"University Community" means all students, alumni, faculty and staff of the University of Baltimore.

"Data Steward" is an employee of the University who oversees the lifecycle of one or more elements of Institutional Data. Charged with ensuring compliance with policy and regulatory obligations, the Data Steward determines appropriate classification of the data, governs its usage, and approves access to it.

“Data Custodian” is an employee of the University who has administrative and/or operational responsibility over Institutional Data. In the course of daily operations and following business rules, data custodians process system transactions that add, append and/or alter data elements.

“Data Classification” is a process that sorts data into categories that identify the necessary level of protection.

“Public Data” are data that are not confidential and can be shared without any implications for the University. Temporary loss of availability is an acceptable risk. The integrity of data is important, but not vital. For the purposes of classification, these data will also be referred to as Category 1.

“Proprietary Data” are data that are restricted to the Data Steward-approved internal access and protected from any unauthorized or external access. An unauthorized access, modification and/or loss of availability, could influence the University’s operational effectiveness, cause financial losses or negatively impact University’s public image. For the purposes of classification, these data will also be referred to as Category 2.

“Confidential Data” are data that are protected by confidentiality agreements, and/or State or Federal laws. An unauthorized access, modification and/or loss of availability, could compromise the identity or financial record of a member of the University Community, impact University’s operational effectiveness, cause a severe financial loss and/or negative impact on University’s public image. The highest possible levels of integrity, confidentiality and availability are vital. For the purposes of classification, these data will also be referred to as Category 3.

“Restricted Data” are data designated as sensitive by law, and require specific management of risks, threats or vulnerabilities. Any compromise in confidentiality, integrity or availability of information could result in severe financial loss, negative impact on University’s public image, and/or result in civil and criminal penalties. For the purposes of classification, these data will also be referred to as Category 4.

III. Scope

This policy applies to all Institutional Data and those who access, process and store it, including all members of the University Community, as well as organizations or individuals handling data on behalf of the University.

IV. Policy

All Institutional Data must be classified with one of the following four classifications: Public, Proprietary, Confidential, or Restricted. A listing of Institutional Data and corresponding classifications will be maintained by the Office of Technology Services. Data Use Standards will be published to the University Community and maintained by the Office of Technology Services.

V. Responsibilities

It is the responsibility of the appropriate Data Steward to evaluate and classify data for which they are responsible according to the classification system established in this policy. All members of the University Community with access to university data are responsible for complying with the requirements outlined in the Data Use Standards. In cases where persons outside of the University Community are given access to data covered by this policy, they must be made aware of this policy may be required to sign a non-disclosure agreement or other document to safeguard the data.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, a student information system will contain a student's directory information as well as their social security number.

Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

VI. Examples of Data Classification

The following are provided as examples of classified data:

Category 1 – Public Data:

- Information available in public domain, including publicly available university websites
- University's brochures and advertisements
- Official financial reports, required by regulatory authorities, which are not classified as Categories 2, 3 or 4
- Newsletters for external dissemination

Category 2 - Proprietary Data:

- Financial information, which is not classified as Category 3 or 4
- Confidential emails
- Data, utilized and collected as part of the research of faculty, students or research centers, which is not classified as Category 3 or 4
- Bulk metadata
- University identified FERPA directory information

Category 3 - Confidential Data:

- Personally identifiable information (PII)
- Personally identifiable education records
- Authentication verifiers
- GDPR-designated personal information
- Contracts that are not classified as Category 4
- Confidential agreements that are not classified as Category 4
- FAFSA

Category 4 - Restricted Data:

- HIPAA-protected records
- Contracts that mandate stricter security
- Payment card information

VII. Related Policies, Standards and Guidelines

- Payment Card Industry Data Security Standard (PCI DSS)
- University of Baltimore Institutional Data Management Policy
- University System of Maryland Board of Regents Directives
- University System of Maryland Information Technology Security Standards
- University System of Maryland Policies

VIII. Legal References

- California Consumer Privacy Act
- Family Educational Rights and Privacy Act (FERPA)
- Free Application for Federal Student Aid (FAFSA)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Higher Education Reauthorization Act
- Maryland State Laws and Regulations