UNIVERSITY OF MARYLAND

UMD Data Classification STANDARD

Purpose

This Standard establishes a framework for the classification of University Data. The UMD Data Classification Standard (the "Standard") serves to augment the requirements of the University of Maryland Policy on Data Management Structure and Procedures - VI-23.00(A) and is enforceable as University Policy. The Standard also provides guidance to assist in determining the baseline security controls necessary to appropriately protect the confidentiality, integrity, and availability of University Data.

The Standard will assist all members of the University community in assessing University Data and information systems on which University Data will be stored, processed, or transmitted; the Data Classification of University Information will determine what level of security is required to protect the University Data. The Standard exists in addition to all other University policies and federal and state laws and regulations.

Definitions

Term	Definition
University Data	*Data which is created, accessed,processed, managed, and/or controlled by the University*
IT System Owner	*The University employee or unit who is responsible for the operation, documentation, security, and maintenance of a University IT system.*

Scope

The Standard is applicable to all University Data that are stored, processed, or transmitted through University resources or other resources where University business occurs. All University Data falls within one of the four categories defined below. Any personal data belonging to the operator of a system that may be stored, processed, or transmitted on a University IT resource as the result of incidental personal use is not considered University Data. Information that is designated "Classified" by the US Government under Executive Order 13526 (at the time of this Standard version) for national security purposes is outside of the scope of this Standard.

Data Classification

The University will use Data Classification to develop Policies, Guidelines and Standards for risk-based protection of information and systems. Data Classifications are based upon the expected risk of harm to individuals and the University if the data were to be subject to unauthorized access, alteration, loss, or disclosure. Harm may encompass negative psychological, reputational, financial, personal safety, legal, and/or other ramifications to individuals or the University. The classification of data determines the baseline security protections and controls that are appropriate. The University's identified/designated IT System Owners are primarily responsible for the implementation of appropriate safeguards and controls, and the safeguards for the highest classification of data applies where multiple classifications of data may exist in one information system. Definitions and basic principles of Data Classification are provided below.

Note that the examples provided are illustrative, rather than exhaustive. The University, faculty, staff, students, and units will interact with many more specific types of data. In the event that a specific type of data is not listed as an example, the Information Classification will be based upon the Definition of each Classification.

DIT must maintain and disseminate a Data Classification Table (below) that specifies the four data risk categories and provides examples of each category. All University Data should be classified into one of the four categories described below:

Information Classification	Definition	Examples
Restricted (Level 4)	Access and use are strictly controlled and restricted by laws, regulations, or contracts. Unauthorized access, use, disclosure, or loss will have significant legal consequences, including civil and criminal penalties, loss of funding, inability to continue current research, and inability to obtain future funding or partnerships.	• Payment Card Industry Data Security Standard (PCI-DSS) Data • Controlled Unclassified Information (CUI) • Export-Controlled Information • Health Insurance Portability and Accountability Act (HIPAA) data
High (Level 3)	Unauthorized access, use, disclosure, or loss is likely to have significant and severe adverse effects for individuals, groups, or the University. These adverse effects could include, but are not limited to, social, psychological, reputational, financial, or legal harm. Compliance requirements are not as strict as for Restricted Information.	• Personally Identifiable Information (PII) as defined in Maryland Code, Commercial Law § 14-3501 • Identifiable data elements that contain sensitive health information that are not otherwise subject to HIPAA
Moderate (Level 2)	Unauthorized access, use, disclosure, or loss is likely to have adverse effects for individuals, groups, or the University, but will not have a significant impact on the University. These adverse effects could include but are not limited to social, psychological, reputational, financial, or legal harm.	• Non-PII student records • Personnel records

Low (Level 1)	Unauthorized access, use, disclosure, or loss is likely to have low or no risk to individuals, groups, or the University. These adverse effects may, but are unlikely to, include limited reputational, psychological, social, or financial harm. Low Risk Information may include some non-public data.	• Data made freely available by public sources • Published data • Educational data • Initial and intermediate Research Data

Data users, in consultation with the appropriate University offices responsible for information security, privacy, and legal compliance, determine the classification of data for which they are responsible using the classification system adopted by the University. IT System Owners must implement systems, data security controls, and compliance measures commensurate with the categorization of the data. If data of more than one level of sensitivity exists in the same system or endpoint, all such data shall be classified at the highest applicable level of security.

Note that compliance with this classification Standard alone is not sufficient to ensure that data will be properly secured. Instead, any data classification should be integrated into a comprehensive IT system security plan that addresses all information resources and devices. All University employees, students, affiliates, and third-party agents who handle University Data must follow these Standards.

Non-Compliance

Non-compliance with these standards may result in adverse impact to UMD's mission, safety, finances, contractual obligations, and/or reputation.

Contact

Division of Information Technology - itsupport@umd.edu

Related UMD and USM Policies

I. http://www.president.umd.edu/sites/president.umd.edu/files/documents/policies/VI-2300A.pdf
II. http://www.usmh.usmd.edu/regents/bylaws/SectionIV/

History

Issued /Approved by ITC: 12/14/2016 - Revised on: 03/10/2021