UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Data Classification	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
APPROVER:	Jacqueline A. Travisano, Ed.D. Executive Vice President for Business and Finance and Chief Operating Officer	SUPERSEDES:	Version 2
		VERSION:	3
		EFFECTIVE:	June 1, 2018

The University of Miami's mission is to educate and nurture students, to create knowledge, and to provide service to our community and beyond. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University leadership and management is committed to safeguarding those resources while protecting and promoting academic freedom. Academic freedom is a core tenet of American research universities.

I. PURPOSE

The University recognizes Data as an asset, and this policy serves to establish a framework for classifying University Data based on its level of sensitivity, value, and criticality to the University. As required by, but not limited to, the University's Information Security Policy, government regulations, and industry standards, classification of Data will aid in determining baseline security standards and controls for protection of the Data.

II. SCOPE

This policy applies to all Users.

III. POLICY

All University Data will be classified according to the Data's sensitivity, value, criticality, and associated risks. The classification of Data shall consist of:

- Identifying, sorting, defining, and assigning each item of Data into one of four classifications: Confidential, Private, Sensitive, or Public; and
- Ensuring adequate and reasonable levels of protection and privacy for all classification levels of Data as required and needed.

IV. DATA CLASSIFICATION STANDARDS

The following Data Classification standards are based on legal and regulatory requirements, ethical considerations, the strategic and proprietary value of Data, and the level of risk resulting to the University from the unauthorized disclosure, alteration, or destruction of Data.

Confidential (Restricted)

Considered the most protected and sensitive of the Data Classification levels and requiring

the highest level of protection and privacy, Confidential Data includes information that the University is under legal or contractual obligation to protect from disclosure, alteration, or destruction. All availability and use of Confidential Data is subject to applicable law, rules, and regulations. The availability and use of Confidential Data is restricted to University-authorized personnel whose job functions necessitate access to such Data; and to third parties and vendors as permitted by the University, by law or pursuant to valid legal inquiries.

The inappropriate and/or unauthorized disclosure, use, alteration, or destruction of Confidential Data could have severe or catastrophic adverse effects on the University and possibly carry significant civil, fiscal, or criminal liability. Confidential Data includes but is not limited to:

- Investment strategies
- Plans or designs
- Medical research technology
- Controversial research topics
- Financial information
- Passwords
- Private encryption keys
- Pin codes
- Donor names and account numbers
- Credit card numbers
- Student information
- Faculty, staff and student employees' Social Security numbers, dates of birth, taxes, bank information, benefits, beneficiaries, and payroll deductions
- Alumni personal information
- PHI (Personal Health Information), patient data, health and medical records
- Medical research data involving PII (Personally Identifiable Information)
- Intellectual property
- Information covered by non-disclosure agreements

Private

Information considered proprietary and critical to the ongoing business continuity and operations of the University, and is restricted and only available to University-authorized personnel, contractors, vendors, and third parties who have a definite need to access such information within their job functions or through the agreements established between the University. The unauthorized disclosure, alteration, or destruction Private Data may seriously impede the University's operations. Private Data includes but is not limited to:

- Salaries
- Research details or results that are not confidential
- Library transactions
- Financial transactions which do not include confidential data
- Educational records required for business and educational purposes within and by the University
- Information required and maintained by the University that is related to a student, faculty, employee (e.g., home phone, home address, ethnicity, marital status, drug test results, etc.)

Sensitive

Information not approved for general or public distribution. For proprietary, ethical, or privacy considerations, access to Private Data must be limited to those who have a need for such data. Unauthorized disclosure, alteration, or destruction of Sensitive Data may result in minor inconvenience to the University. Examples of Sensitive Data include:

- Accounting and financial information not otherwise classified as Confidential Data

(internal use only)
- Business Plans not otherwise classified as Confidential Data (internal use only)
- Internal memos (internal use only)
- Minutes of Meetings (internal use only)
- Internal reports (internal use only)
- Internal departmental websites used for business/educational purposes (internal use only)
- Prospective Student/Applicant information
- Prospective Employee/Applicant information

Public
Information available to anyone without any legal restrictions on access or use. Public Data, if disclosed, would not impact or affect the University in a negative or derogatory manner. Public Data includes:
- Tuition and fees
- Annual reports
- Press statements
- External facing website and social media sites, blogs, etc.
- Employee names, titles, work phone numbers, work address, email addresses

V. PROTECTION OF DATA

Based on the applicable Data classification, Data must be secured and protected according to applicable University policies and procedures by using current industry standards and safeguards to ensure that Data is not subjected to unauthorized use/exposure, disclosure, alteration, or destruction.

Based on University business needs, Data is to be shared only with those who have a definite need or right to access it.

VI. DEFINITIONS

CISO: University's Chief Information Security Officer

Data: All information created, received, maintained, or transmitted by or on behalf of the University to conduct University business.

Data Classification: The process of classifying University data for sensitivity, value, and criticality according to risk as required for satisfying regulatory compliance requirements, University policies, and industry standards and best practices.

Data Owner: A person or entity who has legal rights and administrative control over a single piece or set of data.

Data Custodian: An individual who has administrative and/or operational responsibility over University Data. Only full-time and permanent part-time employees of the University and/or third party vendors approved by UMIT may function as data custodians.

Data Steward: A senior-level employee of the University responsible for overseeing the governance and compliance requirements of one or more sets of University Data.

Intellectual Property: Includes but is not limited to: patents; domain names; logos; industrial designs; ideas; formulas; compositions; inventions (whether patentable or un-patentable and whether or not reduced to practice); know-how; manufacturing and production processes and techniques; research and development information; drawings; specifications; designs; plans; proposals; technical data; copyrightable works; financial and marketing plans; customer and

supplier lists and information; trademarks; geographical indications; trade secrets; and other legal interests recognized or protected as intellectual property under the law.

Health Records: The Data Protection Act of 1998 defines a health record as "Any electronic or paper information recorded about a person for the purpose of managing their health care." This includes a range of different records including but not limited to Personal Health Information (PHI) as defined within this document; care plans, hand-written nursing and medical records; General Practitioner and primary health care team records; outpatient records; examination/test results; monitoring equipment print outs; photographs of the patient; and X-rays.

PHI: Protected Health Information, a subset of Personally Identifiable Information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer or healthcare clearing house; and (2) relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Health Information for Economic and Clinical Health (HITECH) further defines PHI as individually identifiable health information that can be transmitted by or maintained in electronic media, or transmitted or maintained in any other form or medium such as paper and film.

Examples of PHI include but are not limited to: name; address; all elements of dates (except year) directly related to an individual; telephone number; facsimile number; email address; SSN; medical record number; health plan beneficiary number; account number; certificate/license numbers; vehicle identifiers and serial numbers; web universal locator (URL); Internet Protocol (IP) address; biometric identifiers including finger and voice prints; full-face photographic images and any comparable images; and any other unique identifying number, characteristic or code.

PII: Personally Identifiable Information. The National Institute of Standards and Technology (NIST) special publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Examples of different types of PII are identified under these government regulations, including but not limited to:

- HIPAA (Health Insurance Portability Accountability Act)/HITECH (Health Information for Economic and Clinical Health) – Health related information
- GLBA (Graham Leech Bliley Act) – Financial information
- Privacy Act – Fair Information Practices for PII held by Federal Agencies
- COPPA (Children's Online Privacy Protection Act) – Protection of children's privacy by allowing parents to control what information is collected
- FERPA (Family Educational Privacy Rights Act) - Student's personal information
- FCRA (Fair Credit Reporting Act) - Collection and use of consumer information
- GDPR (General Data Protection Regulation) – Personal information related to individuals in the European Union

System Administrator: An individual responsible for the maintenance and protection for any electronic or paper-based system creating, storing, and/or transferring Data.

Users: Individuals who may interact with University Data, including, but not limited to, University trustees, officers, faculty, students, staff, alumni, contractors, vendors, guests, consultants, volunteers, and temporary employees.

University: The University of Miami and all of its units.

UMIT: University of Miami Information Technology

VII. PROCEDURE

Responsibilities:

A Data Owner/Steward/Custodian can serve as a single role, as three individual roles, or any combination of the three. At minimum, there must be a designated data owner. An owner can be the University, a University department, or an individual. Responsibilities include, but are not limited to:

- Appropriately classify University Data.
- Assign administrative and operational responsibilities for University Data.
- Provide oversight and management for the sensitivity, value and criticality of Data according to this policy, related University policies and all applicable regulations and industry standards and best practices.
- According to policy and procedure, determine and implement the criteria for obtaining rightful access to University Data.
- Understand how University Data is governed by University policies, government regulations, contracts, and other legal binding agreements.
- Label Data as classified.
- Implement appropriate technical safeguards to protect the confidentiality, integrity, and availability of University Data.
- Understand and report how University Data is stored, processed and transmitted by the University and by third party vendor(s) or contractor(s).
- Understand and report security risks for University Data.
- Periodically re-evaluate the classification of Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the Data or its value to the University.
- Such other responsibilities as determined by CISO or CISO's designee(s).

Users:

- Adhere to all University policies and procedures pertaining to the classification and protection of University Data.

System Administrator

- Implement appropriate safeguards and controls to maintain compliance with all applicable University policies and procedures for Data.

Reporting a Potential or Actual Violation, Incident, or Breach of this Policy

- Any potential or actual violation, incident or breach of this policy must be reported according to the UMIT Incident Notification Policy and the UMIT Incident Response Policy.

CISO:

- Determine security risks and assess how they may impact University Data.
- Enforce, manage, maintain, and administer this policy.

VIII. SANCTIONS

All allegations of violations of policy will be investigated by the appropriate University administrative offices with the assistance of the University of Miami Information Technology and the appropriate department such as the Human Resources, Student Affairs or the Office of the Provost. Events and incidents determined to be a violation of the policy will be addressed according to applicable disciplinary policies and procedures.

Penalties may include:

- Suspension or termination of account and network access and/or other disciplinary action up to and including termination of employment.
- Criminal and/or civil prosecution.