UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Data Classification	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A110-028-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 March 1, 2017

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the requirements that follow have been identified to promote the best balance possible between information security and academic freedom.

I. PURPOSE:

The University of Miami's mission is to educate and nurture students, to create knowledge, and to provide service to our community and beyond. This policy establishes a framework to classify the University's data from risks including but not limited to, access, use, disclosure, removal, and unauthorized destruction. The University recognizes data as an asset and therefore this policy establishes guidelines for categorizing data based on the sensitivity of the information and regulatory requirements, such as HIPAA, FERPA, and industry compliance PCI.

II. SCOPE:

This policy applies to all electronic data stored on any media or system(s) throughout the University of Miami and applies to all individuals storing, accessing, or working with the data, in any way, including all University employees, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties utilizing University resources.

III. POLICY:

All data shall be classified by the University into levels based on sensitivity and risk. University system administrators, data custodians and/or users will be responsible for assigning each item of institutional data to one of four categories; Confidential, Private, Sensitive, or Public.

Data classification categories:

These categories take into account regulatory requirements, contractual agreements, ethical considerations, and strategic/proprietary worth.

Level 1 – Confidential (Restricted)

Confidential information includes data covered by Federal and State legislation such as FERPA, HIPAA, and the Data Protection Act or is legally covered by contract and must be protected at

all times. The disclosure of this information may seriously damage or negatively impact the University. This information includes, but in not limited to:

- Investment strategies
- Plans or designs
- Medical research technology
- Controversial research topics
- Financial information
- File encryption keys
- Social Security Numbers
- Donor names and account numbers
- Credit card numbers
- Sensitive student information
- Faculty, employee or alumni personal information
- Patient's medical records.

Level 2 –Private

Private information is data restricted to proprietary use by authorized personnel only and is considered critical to ongoing options. The disclosure of this information may seriously impede the University's operations. This information 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
- Information covered by non-disclosure agreements
- Educational records including file documents or other materials
- Information directly related to a student, faculty, employee, and maintained by the University (i.e., home phone, address, date of birth, drug test results, etc.).

Level 3 – Sensitive (Internal Use Only)

Sensitive information is data not approved for general distribution outside the University. Access to this information must be guarded to proprietary, ethical, or privacy considerations. The disclosure of this information may result in a minor inconvenience to the University and its management. Examples of sensitive information include:

- Accounting information
- Business Plans
- Internal memos
- Minutes of Meetings
- Internal reports

Level 4 – Public

Public information is data without any, national or international legal restriction regarding access. Public data is information that anyone within the public domain may access. This information, if disclosed, should not impact the University of Miami. This includes:

- Annual reports
- Press statements
- Internet website, etc.

Details regarding the handling of University Information will reside within the Data Classification Procedures document.

IV. DEFINITIONS:

Data: Data includes all information stored on any electronic media throughout the University of Miami.

Data Classification: The process of categorizing an entity's; electronic data based on value at risk as required for satisfying regulatory compliance requirements.

System Administrator/Data Custodian: A data custodian in an individual with the responsibility of maintenance and protection of data on any given system. Only full time and permanent part-time employees of the University and/or third party vendors approved by IT may function as data custodian.

User: An individual who creates or stores data, and thus is the owner of the information.

University: "University" refers to the University of Miami as a whole and includes all units.

V. PROCEDURE:

System Administrator/Data Custodian:

- Responsible for labeling data into one of the four categories and applying appropriate security controls to ensure adequate protection of the information within their assigned responsibilities.

Chief Security Officer (CSO):

- Responsible for monitoring the enforcement of this policy.

User:

- Responsible for identifying appropriate data classification category.

Sanctions:

Account and network access may be administratively suspended with or without notice by the University when, in the University's judgement, continued use of the University's resources may interfere with the work of others places the University or others a risk, or violates University policy. Knowing violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations must be reported to the applicable System Administrator, who will report as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:

- Suspension of termination of access to computer and/or network sources;
- Suspension or termination of employment, to the extent authorized by other University published policies and procedures;
- Suspension or termination of contract computer and/or network services; or
- Criminal and/or civil prosecution.

Enforcement:

Chief Information Security Officer or Designee (CISO) is responsible for monitoring the enforcement for this policy.