

Data Classification Policy

Effective Date:	Month, ##, 2007
Date(s) Reviewed:	
Date (s) Revised:	

PURPOSE:

This policy establishes a layered framework to secure 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.

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.

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 and risk as required for satisfying regulatory compliance requirements.

Data Custodian: A data custodian is 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 custodians.

POLICY:

All University data shall be classified within three months of creation or acceptance of ownership by the University into levels based on sensitivity and risk. University 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. These categories take into account regulatory requirements, contractual agreements, ethical considerations, and strategic/proprietary worth.

Any data that has not yet been classified, i.e. newly created documents, must be treated as Confidential until it has been properly categorized.

DATA CLASSIFICATION CATEGORIES:

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 is 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; accounting information; business plans; sensitive student information; faculty, employee, or alumni personal information; patient's medical records.

PRIVATE

Private information is data restricted to proprietary use by authorized personnel only and is considered critical to ongoing operations. 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.).

SENSITIVE (*Internal-Use Only*)

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

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.

ENFORCEMENT:

Data Custodian:

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

Chief Security Officer (CSO):

- Responsible for monitoring the enforcement of the policy.