

DRAFT

University of Miami Data Classification Policy

December 19, 2006

TABLE OF CONTENTS

- Section One: Purpose
- Section Two: Definitions
- Section Three: Scope
- Section Four: Policy
- Section Five: Data Classification

I. PURPOSE

The purpose of this policy is to establish guidelines for data categorization and risk mitigation. The practical intent of this policy is to establish a layered framework to secure the University's data. Data is an asset of the University and must be classified by the sensitivity and risks associated with the disclosure of the information.

II. DEFINITIONS

A. Safeguards:

Controls or countermeasures employed to reduce the risk associated with a specific threat, or group of threats. These measures are intended to guarantee the confidentiality, integrity and availability of data at all times.

B: Data Classification:

The categorization of the University's data; Data Classification is based on value, and risk associated with disclosure and regulatory law compliance.

III. SCOPE

This policy applies to any electronic University of Miami data accessible or stored by University employees, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties University resources. This policy also applies to all Data Custodians, or System Administrators of departments or schools, regardless of where the data is stored physically. All users are expected to be familiar with and comply with the terms of this policy. In all cases applicable statutes and regulations that govern either protection or accessibility of institutional records will take precedence over this policy.

IV. POLICY

All University data shall be classified into levels of 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 classifications of data take into account the legal protections (by statute, regulation, or by the data subject's choice), contractual agreements, ethical considerations, or strategic or proprietary worth. The classification assigned, and the related controls applied are dependent on the sensitivity of the information. All University data will be designated as university-internal data for use within the university except when noted otherwise.

V. DATA CLASSIFICATION

Level of Sensitivity

A. CONFIDENTIAL (*Restricted*)

DRAFT

DRAFT

Information protected because of protective statutes, policies or regulations. Confidential Information is data that if disclosed or shared, could seriously impede or negatively impact the University and its operation. This information includes investment strategies, plans or designs, medical research technology, controversial research topics, data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, financial information, and commercially sponsored research. Individual health information, system password, 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, bank accountants' information etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Very strong safeguards must be in place to guarantee the protection of this information.

B. PRIVATE

Private information is normally for proprietary use by authorized personnel only. This information includes salaries, research details or results that are not restricted data, library transactions, financial transactions which do not include restricted data; information covered by non-disclosure agreements, education records including files documents or other materials, information directly related to a student, faculty, employee, and maintained by the University, e.g. home phone, address date of birth, drug test results, etc. Such information should not be copied or removed from the organization's operational control without specific authorization. Strong safeguards should be in place to guarantee the protection of this information.

C. SENSITIVE (*Internal Use Only*)

Sensitive information is data not approved for general circulation outside the University. Access to this information must be guarded due to proprietary, ethical, or privacy considerations. If this data is lost, it will only cause a minor inconvenience to the University of Miami and its management. The disclosure of this information is unlikely to result in any financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings, and internal project reports. Safeguards should be in place to guarantee the protection of this information.

D. PUBLIC

Public information is data in the public domain such as annual reports, press statements etc., which has been approved for public use. It is defined as information with no local, national or international legal restriction regarding access. This information, if disclosed, should not impact the University of Miami. Sufficient protection must be applied to prevent unauthorized modification of such data.

DRAFT