Policy # 56003

DATA CLASSIFICATION POLICY

Effective Date: June 19, 2009 **Review Date: January 1, 2022**
Responsible Office: Information Technology Center
Division: Operations

I. PURPOSE/OBJECTIVE

To protect the confidentiality, integrity and availability of university data and to comply with local, state and federal regulations regarding privacy and confidentiality of information in compliance with The Office of Information Technology's ITB 08-02.

II. STATEMENT OF POLICIES

All m embers of the university community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

A. RESPONSIBILITY FOR DATA MANAGEMENT:

Departments are responsible and should carefully evaluate the appropriate data classification category for their information.

B. DATA CLASSIFICATIONS

Data owned, used, created or maintained by the University is classified into the following three categories: Public, Official Use Only and Confidential.

1. Public Data is information that may or must be open to the general public. It is defined as information with no existing local, state, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community

2. Official Use Only Data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from

unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Official Use Only Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data. Official Use only data must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure, must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use, must not be posted on any public website, and must be destroyed when no longer needed subject to the University's Records Management Policy and electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with the OIT's IT POL 1-04 Data Sanitization Policy.

3. Confidential Data is information protected by statutes, regulations, University policies or contractual language. Department Heads may also designate data as Confidential. Confidential Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the University should be authorized by executive management and/or the Vice President. Confidential data when stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided by the Information Technology Center (ITC) in order to protect against loss, theft, unauthorized access and unauthorized disclosure, must not be disclosed to parties without explicit management authorization, must be stored only in a locked drawer or room or an area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, when sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location, must not be posted on any public website. Destruction may be accomplished by "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste and electronic storage media shall be sanitized appropriately by degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with OIT's IT POL 1-04 Data Sanitization Policy.

The ITC Security Administrator must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

C. DATA CLASSIFICATION ROLES AND RESPONSIBILITIES

1. The Information Technology Center is the primary entity charged with developing policy and procedures subordinate to and in support of this policy.

2. The ITC Security Administrator is charged with the promotion of security awareness within the University community, as well as responsibility for the creation, maintenance, enforcement and design of training on relevant security standards in support of this policy.

3. The ITC Security Administrator will receive and maintain reports of incidents, threats and malfunction that may have a security impact on the University's information systems, and will receive and maintain records of actions taken or policies and procedures developed in response to such reports. The ITC Security Administrator will assist the Internal Audit Department, as appropriate, in conducting periodic audits to determine University compliance with this policy.

4. The Information Technology Center will facilitate distribution of this policy, will assist in the investigation of policy breaches, and administer a confidential method for reporting instances of suspected misconduct, violations of law or University policies.

5. The University's Executive Cabinet will review procedures issued under authority of this policy f or compliance with applicable regulations. General Counsel will also respond to court ordered releases of information. The Information Technology Advisory Council will be the initial forum for discussion of questions arising out of or in response to this policy.

D. VIOLATIONS

Violations of this policy can lead to disciplinary action up to and including dismissal, expulsion, and/or legal action. Any known violations of this policy are to be reported to the university's Associate Vice President for Information Technology or the Information Technology Center's Security Administrator.

III. REVISION/REVISED HISTORY

June 19 2009-Effective Date