INFORMATION MANAGEMENT and CLASSIFICATION STANDARD

University of Louisville data is a critical university resource and asset. It often contains information about the University, as well as personal information about faculty, staff, students, patients and other affiliated parties. Protection of this information may be required by federal, state, industry or other agency regulations or it may be driven by financial, reputational, legal or other university requirements. The Information Management and Classification Standard establishes procedures and guidelines to ensure university information assets are identified, receive an appropriate level of protection and that those with access to university assets make appropriate decisions regarding their use and security.

Responsibilities:

It is the responsibility of each individual to ensure the security and protection of university information assets (data, systems, electronic or hardcopy) they own, control or use. Assets should be identified, classified and the appropriate degree of protection applied based on its use, sensitivity and importance to the University and in compliance with all regulations, laws or university policies.

Classification - Sensitivity:

University information assets, whether physical or electronic, are either sensitive or non-sensitive. Sensitive can be further classified among one of three categories: "*Confidential*," "*ProprietaryInternal Use Only*," and "*Public*." Where practical, all data is to be explicitly classified, such that users of any particular data received or derived from an information resource are aware of its classification. Assets that are not classified are considered to be *Proprietary* unless under regulation or until determined otherwise. Sensitivity categories are further defined below.

 ***Sensitive**:*

- **Confidential** information includes sensitive personal and/or university information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or university policy. Unauthorized access to *Confidential* information may result in a significant invasion of privacy, may expose the University to significant financial risk, or result in negative impacts on the operations, or reputation of the University. Examples of confidential information include: information protected under regulations such as, FERPA, HIPAA, HB-5, PCI-DSS, and the Gramm-LeachBliley Act, personally identifiable medical and health information, grades and other enrollment information, credit card, bank account and other personal financial information, social security numbers, grant reviews, research data, dates of birth (when combined with name, address and/or phone numbers), employee ID (when combined with first name or first initial and last name) user IDs when combined with a password, university financial and planning information, legally privileged information, and other information concerning research or pending patent applications.

- **Proprietary-Internal Use Only** information includes information that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on interests, or on the finances, operations, or reputation of the University. Examples of this type of data include internal memos meant for limited circulation or draft documents prior to public release.

***Non-Sensitive**:*

- **<u>Public</u>** information is information that is generally available to the public, or that, if it was to become available to the public, would have no material adverse effect on the University community or upon the finances, operations, or reputation of the University.

Controls - Sensitivity (Labeling and Handling):

Controls for labeling and handling (storage, transmission, distribution and disposal) of information assets are defined based upon confidentiality classification level. Examples of controls include: encryption, secure disposal (shredding or wiping) and document labeling. When more stringent, adherence to regulatory controls is required. There are no restrictions on public information. It is the responsibility of all users to adhere to the control guidelines per the *Information Classification and Handling Guide*.

Classification – Integrity and Availability:

In addition to sensitivity classifications, university information assets should also be assigned an integrity and availability classification indicating the degree of data accuracy, validity, and availability required as defined by the University's *Information Management and Classification Glossary*. Integrity classifications include High, Medium and Low. Availability classifications include required system availability times such as 24/7, 12/5, best effort, redundancy, tape.

Controls – Integrity and Availability:

Protective controls such as approval and monitoring of access, authentication, encryption, logging and monitoring, audit controls, backup, and DR processes should be consistent with the asset's integrity and availability requirements. See *Information Integrity and Availability Guide.*