**Classification and Use of Information Assets D 101**

**SCOPE**

This policy applies to the creation, collection, classification, use, and retention of electronic information for academic, research, and administrative purposes.

**POLICY**

As a routine matter, data in electronic form is created, collected, used and maintained by members of the University community for educational, research, public service and health care purposes. Each person with access to University data shall comply with applicable data protection and control procedures, and shall secure that data against inappropriate, unauthorized or illegal use.

1. Assessment of the inventory of information assets is a critical step in protecting those elements that need special handling. The inventory includes assessments based on general personal information (ID Theft), those elements protected by FERPA and HIPAA where applicable, and data that must be restricted based on Gramm-Leach-Bliley (GLB).
   
   A. The Security Steering Committee will specify the composition of sub-groups that will take responsibility for the inventory. These groups will be authorized by the Steering Committee to conduct the inventory.
   
   B. Data elements are to be classified as public, private or sensitive based on applicable laws, University policies, and potential reputational damage that may occur should the data be compromised.
   
   C. Identified data elements will be further classified by the applications that need them to meet the educational and business needs of the University.
   
   D. Classification of the data element will include combinations of data. For example, a Social Security number by itself has no intrinsic value. However, combined with other data elements like name, address, date of birth, raise the level of sensitivity. Applications that contain these combinations of data elements must be classified to afford the highest level of protection.

2. **Data Stewardship:** The Chief Information Officer (CIO) and designated data custodians for each office of record shall ensure that University data is created, used, maintained, disclosed and disposed of according to applicable law, regulation or University policy. See DoIT 100.

   A. Data custodians shall develop appropriate access controls to data in the department, division or unit under their supervision, consistent with the data’s confidentiality, sensitivity and use. As a general matter, stewardship for: student records information resides with the Office of Registrar; Admissions data resides with the Director of Enrollment Management; Graduate Students data resides with the Graduate School in consultation with School of Professional Development, Health Sciences Center, or the School of Medicine; employee information resides with Human Resources; financial aid resides with the Financial Aid Office; medical information resides with Health Information Management, alumni and donor data resides with the Vp for Advancement, and University information resides with the Public Information Officer.

   B. Disclosure or distribution of University data is prohibited unless authorized in writing by the Information
Security Team in consultation University counsel. The University maintains audit trail records in accordance with legal requirements, the needs of the University’s Internal Audit Department and disaster recovery procedures.

3. **Data Retention**: DoIT maintains electronic backups of data as specified in DoIT Policy D111 Electronic Data Retention.

4. **Data Security**: All transmissions of confidential data shall be over a secured channel or be encrypted.

   Each employee who may have access to confidential information shall, as a condition of employment, sign an Information Security Compliance Agreement, which shall be included in the employee’s personnel record.

   Managers shall promptly report changes in employee job status or duties involving data access to the appropriate data custodian and to the Office of Computer Accounts.

   Generally, disclosure of confidential information, including, by way of example only, personnel, student, financial and patient information is prohibited by law. Access to this data is available only to persons with a “need to know” by virtue of their job responsibilities, in accordance with law, or an authorized request.

   Data Exchange Agreements with state, local or federal agencies and any lease, permit or contract with a third party that may involve access to University data shall include a statement of compliance with University policies on data security and confidentiality. All Data Exchange Agreements must be approved by the appropriate data custodian and the Information Security Committee.

5. **Physical Security**: All computers, data storage media and storage repositories that contain confidential information must be secured against loss or tampering.

   Portable computing devices such as laptops, hand-held equipment (PDAs) and data storage media pose a significant risk for the exposure of protected information and potential access to the University’s administrative systems. For these reasons, special care must be exercised when utilizing these devices. All protected data stored on portable devices must be encrypted. In addition, the login settings for these devices should never be set for automated login to any University administrative application.

   All administrative systems shall have and document backup and recovery procedures. The backup media must be stored in a secure location off site. DoIT shall test these procedures on a periodic basis.

6. **Penalties for Misuse**: The inappropriate or illegal use of University data is a violation of University policy that will subject the violator to disciplinary procedure. Individuals that misuse University information technology resources may lose information technology privileges and be referred for prosecution by state or federal authorities.

**INQUIRIES/REQUESTS:**

Office of the Chief Information Officer  
Room 231, Educational Communications Center  
632 – 9085  

Office of Institutional Research  
Room 310, Administration Building  
632 – 7272