Information Classification and Protection Policy

1.0 Purpose

Students, faculty, staff, and alumni trust that the University protects their personal information as it exists in any medium – electronic, as well as all forms of paper record. This policy is designed to help each member of the University community do his or her part to fulfill that trust. This policy defines how University information is classified and how it is to be protected.

2.0 Applicability

All University faculty, staff, and students shall comply with this policy and any management controls derived from it, as they acquire, communicate, transmit, process, or store information on behalf of the University. The University shall also require that third parties handle University information in accordance with applicable laws and regulations and accept liability for violation of those laws and regulations for any University information that they acquire, communicate, transmit, process, or store on behalf of the University.

3.0 Policy

Managers in the schools and divisions shall periodically inventory all information their offices acquire, communicate, transmit, process, or store and assign it to one of the information classifications defined in this policy. The managers shall then apply and document the appropriate controls for each set of records (e.g. forms, electronic document, database, etc) based on the highest classification of data contained in those records (see currently supported controls in Appendix C and classification / documentation examples in Appendix D).

University information is contained in physical or electronic records. Physical records (which includes all forms of paper records and documents) contain information directly readable by humans. Electronic records contain information that requires an electronic device to read the information. Managers shall inventory information regardless of record type.

4.0 Classifications

Information shall be classified in one of the following categories.

4.1 Restricted information is University information that:

- includes authentication secrets (passwords, private keys; See Schedule A for further examples);
- makes the University liable for costs or damages due to unauthorized disclosure under laws, government regulations or contract;
- pertains to information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). See Schedule A for further information.

4.2 Confidential information is University information that:

- is used primarily to conduct official University business with limited internal distribution;
- contains proprietary information, or pertains to student records that are covered by the Family Educational Rights and Privacy Act (FERPA). See Schedule A for further information.

4.3 Public information is University information that:

- is not classified as restricted or confidential.

5.0 Controls

The appropriate control shall be applied to every process used to handle information, according to the classification of that information.

5.1 Acquisition

Restricted and Confidential information shall only be requested from an individual, or acquired from other sources, when there is a legal and active business use for the information.

5.2 Access

For Restricted and Confidential information, in any medium, University managers shall use appropriate physical and electronic controls to limit access to this information to persons who need to use it to perform their University assigned duties and for whom it is legally appropriate to have access to this information. For restricted information, it is required that those given access have a need to know and have executed a non-disclosure/confidentiality agreement that covers this information.

Information Classification and Protection Policy

5.3 Network Transmission

Confidential information may be transmitted over the University or external networks as required, provided that access to the information by normal means is restricted to those who must use it to perform University assigned duties.

Restricted information shall not be transmitted over University or external networks, outside a data center, a firewalled network so designated by Information Technology, unless the data or the entire transmission is encrypted. Questions regarding encryption of data for external transmission should be directed to the Information Security Office prior to transmission.

5.4 Data Processing

The University and its employees shall employ data processing systems and procedures with appropriate safeguards to ensure that Restricted and Confidential information is not lost or disclosed to unauthorized persons during or after processing.

5.5 Communication

Confidential and Restricted information communicated by voice, mail, fax, or other methods must use reasonable safeguards against disclosure to unauthorized persons, as appropriate to the method of communication.

Restricted information may not be communicated to third parties, except as specifically required by legal obligation or protected under contractual agreements.

5.6 Storage

Confidential information shall be stored in physical or electronic environments where access is limited to only those who need to use the information for University assigned duties and for whom it is legally appropriate to have access to this information.

Restricted information in electronic records shall be secured with strong encryption when stored outside the central University administrative database. Restricted information in all forms of physical records must either be securely locked or actively supervised in a private environment at all times.

5.7 Retention, Disposal and Transfer

Confidential and Restricted information must be retained and disposed of in accordance with the University's Records Management Policy. Computers and other electronic devices must be transferred or disposed of in accordance with the Computer Disposal Policy.

6.0 Improper Disclosure or Loss

All faculty, staff, and students shall immediately report inappropriate disclosure or suspected loss of Confidential or Restricted information to their supervisor or IT Help Desk. The supervisor or IT Help Desk shall inform the Information Security Office promptly when loss or improper disclosure of records containing Confidential or Restricted information is suspected or confirmed.

The responsible division head or dean will sign any legally mandated information breach notification letters for information lost or disclosed by their employees.

7.0 Assistance

The Information Security Office shall maintain a matrix of applicable controls by process and information type for use by managers and technical advisors. This matrix shall be considered Schedule B of this policy. A list of recommended technical procedures for implementing encryption and access controls will be maintained by Information Technology and published by the Information Security Office, considered Schedule C of this policy.

For consulting on classification and control of electronic information, contact the Information Security Office. Information on the classification and control of physical records is available from Risk Management.

8.0 Enforcement

Failure to comply with this policy may result in discipline, suspension, dismissal and/or legal action.