DATA CLASSIFICATION GUIDE

NOTE: For the purposes of this document, the terms "data," "information," and "records" are synonymous.

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by federal law, state law, Texas State University System Rule and Regulations, university policy, as well as proprietary, ethical, operational and privacy considerations.

Prior to releasing, publishing, or disclosing any information, the information owner information shall classify the information according to one of the three levels outlined below.

The information owner shall ensure that disclosure controls and procedures are implemented to afford the degree of protection required by the assigned classification.

Higher education and industry best practices suggest the need for three classifications with respect to data confidentiality. In order from least to most confidential, these are:

a. Public (Level 1) Information

Public information is by its very nature designed to be shared broadly, without restriction, at the complete discretion of the information owner. It may or may not have been explicitly designated as public. There is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm to the university, individuals, or affiliates. From the perspective of confidentiality, public information may be disclosed or published by any person at any time.

Examples: advertising, degree program descriptions, course offerings and schedules, campus maps, published research (within copyright restrictions), job postings, press releases, general information about university products and services, certain types of unrestricted directory information as specified by the Family Educations Rights and Privacy Act of 1974 (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA).

b. Sensitive (Level 2) Information

Sensitive information is the most difficult to describe as it often presents attributes of both Public and Confidential information. Sensitive information is often considered “public” in the sense that it is releasable under provisions of the Texas Public Information Act, while also requiring assurances that its release is both controlled and lawful. Sensitive information is often intended for use within a specific workgroup, department or group of individuals with a legitimate need-to-know. Likewise, access to Sensitive information is often controlled by identity

authentication and authorization measures (e.g., LoboID and password). Unauthorized disclosure of Sensitive information could adversely impact the university, individuals or affiliates.

Examples: some employee records (such as performance appraisals, dates of birth, etc.), departmental policies and procedures that might reveal otherwise restricted information, the contents of e-mail, voicemail, instant messages and memos, unpublished research, information covered by non-disclosure agreements, donor information, etc.

Generally speaking, Sensitive information should not be published or disclosed to the public except by the university's designated owner of the requested information in accordance with the owner's established procedures for processing TPIA requests, or as otherwise authorized by IT Security or the TSUS Associate General Counsel. (See separate list of the university's designated information owners)

c. Confidential (Level 3) Information

According to Chapter 202 of the Texas Administrative Code (TAC 202), Confidential information is "information that is excepted from disclosure requirements under the provisions of applicable state or federal law" such as the Texas Public Information Act (TPIA) and the Family Education Rights and Privacy Act (FERPA). Confidential information presents the most serious risk of harm if improperly disclosed. Confidential information is generally intended for a very specific purpose and should not be disclosed to anyone without a demonstrated need-to-know, even within a workgroup or department. Disclosure of Confidential information is generally regulated by specific legal statutes (e.g., TPIA, FERPA, HIPAA), published opinions by the Office of the Attorney General of Texas, the Texas State University System Rules and Regulations, or contractual agreements. Unauthorized disclosure of this information could have a serious adverse impact on the university, individuals, or affiliates.

Examples: student education records as defined under FERPA, credit card information, bank account numbers, social security numbers, driver license numbers, personally identifiable medical records, passport information, crime victim information, library circulation records, court sealed records, access control credentials (e.g., PINs and passwords), etc.

Confidential information must not be published or disclosed to the public under any circumstances other than those specifically authorized by law. Any such disclosure should be immediately reported to the CIO for damage mitigation and investigation. Requests for such information received from persons with a

questionable need to know should be directed to the TSUS Associate General Counsel.

Standards for Handling Confidential Information

Because of the harm that can result from improper disclosure, confidential university information shall be afforded the following special protections by owners, custodians, and users:

a. A person's social security number, driver license number, or other widely-used government-issued identification number shall not be captured, stored, or used as a person identifier unless such use is required by an external, governmental, or regulatory system that is authorized for use at the university. The LoboID or A-number should be used in lieu of such prohibited identifiers in situations where personal names or other identifiers do not assure uniqueness. Where use of such numbers is required, owners, custodians, and users shall store these numbers in encrypted form, when possible, or use other compensating controls with the advice and authorization of the ISO.

b. Payment cardholder data (i.e., the primary account number or the magnetic stripe contents together with any one of: cardholder name, expiration date, or the service code) shall not be stored on any device connected to the university's data network for longer than is necessary to authorize a transaction using that information.

c. Confidential information must not be transmitted electronically over a public network (e.g., the Internet) in unencrypted form. Either the information itself must be encrypted prior to transmission or an encrypted connection must be established and maintained for the duration of the transmission. Authorized encrypted connection examples include the university's implementations of: VPN – Virtual Private Network, TLS – Transport Layer Security, and SSH – Secure Shell.

d. Confidential information must not be stored on portable devices or media such as notebook or tablet computers, PDAs, smart phones, USB drives, CDs, DVDs, tape cartridges, etc. If such storage is required, the confidential information must be protected by encryption or by other compensating controls with the advice and authorization of the ISO.

e. Confidential information must not be accessed from remote locations in an unauthorized manner. Examples of authorized remote access solutions include the university's implementations of: VPN, TLS, and SSH. Contact OIT for up-to-date information about the acceptability of other remote access solutions.

f. Confidential information should not be stored on personally-owned devices or media. If such storage is required, the confidential information must be protected by encryption or by other compensating controls with the advice and authorization of the ISO.

g. Confidential information must not be stored on any devices external to the campus network except as provided under contract with an authorized information resource service provider that is contractually bound to properly protect the information.

h. Encryption requirements for information storage and transmission, as well as for portable devices, removable media, and encryption key management, shall be based on documented risk management decisions. Contact OIT for up-to-date information about university-supported encryption solutions.

i. Confidential information must not be shared, exposed or transmitted via any peer-to-peer (P2P) file sharing mechanism prior to completion of a comprehensive risk assessment, including penetration testing, of the proposed P2P file sharing mechanism by OIT.