

DATA CLASSIFICATION – BASIC BEST PRACTICES

Distributed at the *Appropriate Release of Information* workshop, April 17 & 18, 2008.

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

1. Prior to releasing, publishing, or disclosing any information, the owner of the information should classify the information according to its need for confidentiality (PUBLIC, SENSITIVE, or RESTRICTED/CONFIDENTIAL, as described in 3 below).
2. The owner of the information should ensure that disclosure controls and procedures are implemented to afford the degree of protection required by the assigned classification.
3. Higher education and industry best practices suggest the need for three classes, or levels, with respect to data confidentiality. In order from least to most confidential, these are:

- a. Public (Level 1) Information

Public information is information that by its very nature is designed to be shared broadly, without restriction, or at the complete discretion of the 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 FERPA and HIPAA, etc.

- b. Sensitive (Level 2) Information

Sensitive information is the most difficult to describe as it often presents attributes of both Public and Restricted/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., NetID 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, and email addresses), 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 University Attorney. (See separate list of the University's designated information owners)

c. Restricted/Confidential (Level 3) Information

According to Chapter 202 of the Texas Administrative Code (TAC 202), Restricted/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). Restricted/Confidential information presents the most serious risk of harm if improperly disclosed. Restricted/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 Restricted/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, Texas State University System rules, or contractual agreements. Unauthorized disclosure of this information could have a serious adverse impact on the University, individuals, or affiliates.

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

Restricted/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 IT Security for damage mitigation and investigation. Requests for such information received from persons with a questionable need to know should be directed to the University Attorney.