UTSA Institutional Compliance Office of Information Security

OIS 9 – Standard for Data Classification

I. STANDARD STATEMENT

The increase in technology enhancements, affordability of portable devices and increased ability to transmit data on demand increases the risk of losing or inadvertently disclosing data. The operation and mission of the University rely heavily on the accuracy, integrity and usability of its data.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. UTSA faculty, staff and other employees are responsible for the security of university data they access, process, transmit and store. UTSA Data Owners must first identify the data they use and classify the data according to the risk categories outlined in the Data Classification Guidelines.

Category I – Confidential	Data whose disclosure, destruction, display, or modification would violate state or federal laws or regulations, UT System policies or the Texas Open records Act.
Category II – Controlled	Data not otherwise protected identified as *Confidential* data, but which are releasable with the Texas Public Information Act. Data protected to ensure a controlled release.
Category III – Published	University data that have no requirement for confidentiality, integrity, or availability. Published (aka Public) data, while subject to UTSA disclosures rules, is available to the UTSA community and all external individuals and entities.

1. University data shall be:
   a. Identified as to its classification - Confidential, Controlled or Published Data - by the Data Owner
   b. Protected in a manner commensurate with its value or category
   c. Appropriately secured against unauthorized creation, updating, processing, destruction and distribution

2. Data Classification

   a. Applies to all data created and maintained by all campuses, except where superseded provisions of a grant, contract or by Federal copyright law.
   b. Applies to all authorized users of the University's computing resources.
   c. Complies with applicable Federal and State laws which govern the privacy and confidentiality of data

3. Classification Categories
   a. All institutional data, on paper as well as in electronic format, must be categorized into one of three levels, Confidential, Controlled, and Published Data. More information about each category is available in the Data Classification Guideline.
   b. The table below outlines standing risks to the university pending breaches of data based on their category.

	Category I	Category II	Category III
Risk to the university should a breach occur	Long-term loss of reputation, long-term loss of critical campus services, long-term loss of research funding, tampering with research, unauthorized exposure of litigation materials, identity or credit theft.	Short-term loss of reputation, short-term loss of research funding, short-term loss of departmental services, Unauthorized tampering with research	Loss of data with no impact to the university, inaccurate general information