The University of Texas Rio Grande Valley
Information Security Office

DATA CLASSIFICATION STANDARD

Table of Contents

1. Purpose

This standard serves as a supplement to the UTRGV AUP (Acceptable Use Policy), which was drafted in response to Texas Administrative Code 202 and UT System UTS-165. Adherence to the standard will facilitate applying the appropriate security controls to university data.

The objective of this standard is to assist data stewards, custodians, and IT owners in the assessment of information systems to determine what level of security is required to protect data on the systems for which they are responsible. The standard divides data into three categories types:

- **CONFIDENTIAL** (historically referred to as Category I)
- **CONTROLLED** (historically referred to as Category II)
- **PUBLISHED** (historically referred to as Category III)

This standard exists in addition to all other university policies and federal and state regulations governing the protection of the university's data. Compliance with this classification standard will not ensure that data will be properly secured. Instead, this standard should be integrated into a comprehensive information security plan.

2. Scope

All university data stored, processed, or transmitted on university resources or other resources where university business occurs must be classified into one of the three categories. Based on the data classification you determine for your system, you are required to implement appropriate technical security measures to protect the data consistent with the university Minimum Security Standards. Confidential data has more stringent requirements than Controlled and Published classifications. All systems require some protective measures.

Note: Data that is personal to the operator of a system and stored, processed, or transmitted on a university IT resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.

3. Audience

All faculty, staff, student employees, contractors, and vendors working with University of Texas Rio Grande Valley data.

4. Data Classification Standard

To classify your data, you must start by understanding what the classifications are. There are specific laws and regulations that govern specific types of data. Additionally, there are situations where you must consider whether the confidentiality, integrity, or availability of the data is a factor. Finally, consider that you may be storing information on more than one system, such as moving data between computers by CD or flash drive, for example. If you rate only your primary computer as Confidential, but not your secondary computer or the transfer media, the secondary computer could put data at risk because it won't be well protected.

4.1. Confidential Data

Confidential university data is protected specifically by federal or state law or University of Texas rules and regulations (e.g., HIPAA; FERPA; U.S. Export Controlled information; Sarbanes-Oxley, Gramm-Leach-Bliley; the Texas Identity Theft Enforcement and Protection Act; University of Texas System Policies; specific donor and employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.) See the extended list of Confidential data classification examples for specifics."

Cause and Effect of Confidential Data	
Examples of How Data Can Be Lost	**Impact of Confidential Data Loss**
• Laptop or other data storage system stolen from car. • Research Assistant accesses system after leaving research project because passwords aren't changed. • Unauthorized visitor walks into unlocked lab and steals equipment or accesses unsecured computer. • Unsecured application on a networked computer is hacked and data stolen.	• Long-term loss of research funding from granting agencies. • Long-term loss of reputation. Published research called into question because data is unreliable. • Unauthorized tampering of research data. • Increase in regulatory requirements. Long-term loss of critical campus or departmental service. • Individuals put at risk for identity theft.

Protect your Confidential data by applying the appropriate Minimum Security Standards.

4.2. Controlled Data

Controlled university data that is not otherwise identified as Confidential data, but which is releasable in accordance with the Texas Public Information Act (e.g., contents of specific e-mail, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release.

Cause and Effect of Controlled Data	
Examples of How Data Can Be Lost	**Impact of Controlled Data Loss**
• In addition to the above scenarios: ○ Staff member wanting to be helpful releases information they are not authorized to share.	• Short-term loss of reputation. • Short-term loss of research funding. • Short-term loss of critical departmental service. • Unauthorized tampering of research data. • Individuals put at risk for identity theft.

Protect your Controlled data by applying the appropriate Minimum Security Standards.

4.3. Published Data

University data not otherwise identified as Confidential or Controlled data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability.

Cause and Effect of Published Data	
Examples of How Data Can Be Lost	**Impact of Published Data Loss**
• See the above scenarios.	• Loss of use of personal workstation or laptop. • Loss of personal data with no impact to the university.

Protect your Published data by applying the appropriate Minimum Security Standards.

5. Non-Compliance and Exceptions

Non-compliance with these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit or Compliance.

University of Texas Rio Grande Valley employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas Rio Grande Valley employees are required to comply with state laws and regulations.

6. Related UTRGV Policies, Procedures, Best Practices and Applicable Laws

The policies and practices listed here inform the system hardening procedures listed in this document; you should be familiar with these documents. (This is not an all-inclusive list of policies and procedures that affect information technology resources.)

UT System (UTS 165) Information Resources Use and Security Policy
UTRGV (AUP) Acceptable Use Policy
Computer Security Standard
Extended list of confidential data
Data Classification Guide
Data Protection Standard for Personally Owned Mobile Devices

7. Revision History

Revision History			
Version	**Date**	**New**	**Original**
1.0	2/16/2017	Created document	Entire document has changed.
2.0	03/20/2017	Revised document	Grammar errors corrected.

8. Sources

UT – Austin Information Security Office (https://security.utexas.edu/)

9. Approvals

Approvals		
Name	**Role**	**Date**
Thomas Owen	Approval	4/13/2017