The University of Texas Rio Grande Valley
Information Security Office

Faculty Data Classification Standard

Table of Contents

Contents

Faculty Data Classification Standard

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 category types:

- **RESTRICTED / CONFIDENTIAL**
- **INTERNAL / CONTROLLED**
- **PUBLIC / PUBLISHED**

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. Definitions

Data User is any person who has been authorized by the owner of the information to read, enter, or update that information. The data user has the responsibility to use the resource only for the purpose specified by the owner, comply with controls established by the owner, and prevent the unauthorized disclosure of confidential data.

Data Stewards are responsible for managing and overseeing the data within their domain. They ensure that data is properly classified, protected, and used in accordance with university policies and regulations.

Custodians are responsible for the technical environment where the data resides. They implement and maintain the security controls to protect the data, ensuring that it is stored, processed, and transmitted securely.

IT Owners are responsible for the overall management and oversight of the information systems that store, process, or transmit university data. They ensure that the systems comply with university policies and standards, and they coordinate with data stewards and custodians to protect the data.

Principal investigator (PI) is the lead researcher for a research project, typically in academic or clinical settings. They are responsible for the overall conduct of the research, including the design, implementation, and reporting of the study. The PI ensures that the research is conducted in compliance with relevant regulations and policies.
Research Assistants: Research assistants support academic research projects by assisting with data collection, analysis, and other research-related tasks. They work under the supervision of a principal investigator.

3. 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. Restricted/Confidential data has more stringent requirements than Internal/Controlled and Public/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.

4. Audience

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

5. 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 Restrictive / 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.

5.1. Restrictive / Confidential Data

Restrictive / 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 or specifics."

Restricted University data includes, but is not limited to, data that is protected by:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Controlled Unclassified Information (CUI)

Data Storage Locations for Restricted / Confidential Data

Data Storage Service Locations	**FERPA**	**HIPAA**	**GLBA**	**SSN**
UTRGV Employee 365 E-mail	Yes	Yes[1]	No	No
UTRGV Isolon Storage	Yes	No	Yes	No
UTRGV Owned Server	Yes[1]	Yes[1]	Yes[1]	With Approval[1]
UTRGV Researcher MS SharePoint, Teams & Onedrive	Yes[1]	Yes[1]	Yes[1]	With Approval[1]
UTRGV Computer	Yes[1]	Yes[1]	Yes[1]	Yes[2,3]
UTRGV Mobile Phone	Yes[1]	Yes[1]	Yes[1]	No
UTRGV Owned NAS Storage	Yes[1]	No	No	No
Other non-UTRGV Storage	Must follow the Security Exception Process			
Non-central IT supported cloud storage	Must follow the Security Exception Process			
Student owned personal device	Please reference Data Classification Standard for Students			

(1) It is assumed that appropriate Access Controls have been enabled and reviewed to ensure that access to data is limited to appropriate individuals. Additional consultation with University Data Stewards and the Information Security Office may be necessary to store data in some locations.

(2) Data can be stored in this location with appropriate and approved controls enabled and approval from the Data Owner and the ISO.

(3) Storage of SSNs is permissible on UTRGV computers if it's part of your official duty and the device meets all security standards, including appropriate encryption technology, as defined and approved by the Information Security Office.
(4) Storage of PCI data is not specifically referenced above as it is not authorized regardless of the data classification.
(5) Other regulated data must be reviewed prior to storage with the ISO to ensure that it is in a secure and compliant environment.

5.2. Internal / Controlled Data

Internal/Controlled university data that is not otherwise identified as Restrictive / 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.

Internal/Controlled Data includes, but is not limited to:

- Internal Communications: Emails, memos, and other communications within the university.
- Research Data: Preliminary research findings and data that are not yet published.
- Course Materials: Lecture notes, syllabi, and other educational resources shared within the university.
- Grant Proposals: Documents detailing research funding requests and project plans.

Data Storage Locations for Internal / Controlled Data

Data Storage Service Locations	Internal / Controlled Data
UTRGV Isolon Storage	Yes
UTRGV Owned Server	Yes
UTRGV Researcher MS SharePoint, Teams & Onedrive	Yes
UTRGV Computer	Yes
UTRGV Mobile Phone	Yes
Personal Computer	Yes
Non-IT Managed Cloud Service	Yes
UTRGV Owned NAS Storage	Yes

5.3. Public / Published Data

Published information encompasses all data not otherwise identified as Restrictive/Confidential or Internal/Controlled data, that has been disseminated to the public domain through various channels, including publicly accessible websites, electronic mailings, social media platforms, printed literature, and other forms of mass communication.

Examples of Public/Published Information Include:

- Statistical analysis and official reports
- Peer-reviewed and publicly accessible research publications
- Institutional or organizational policy documents
- News articles and official press statements
- Publicly available directory data without access restrictions
- Open-access educational materials and resources

Data Storage Locations for Public / Published Data

Data Storage Service Locations	**UTRGV affiliates and public with a "need to know"**
UTRGV Employee 365 E-mail	Yes
UTRGV Isolon Storage	Yes
UTRGV Owned Server	Yes
UTRGV Researcher MS SharePoint, Teams & Onedrive	Yes
UTRGV Computer	Yes
UTRGV Mobile Phone	Yes
Personal Computer	Yes
Non-IT Managed Cloud Service	Yes
UTRGV Owned NAS Storage	Yes
Other Storage	Must follow the Security Exception Process

6. 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 Office of Institutional 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.

If any of the requirements contained within this standard cannot be met, a specific user case and supported documentation must be documented and submitted via the Security Exception Process to address any associated risk. Please note that submission of a Security Exception request does not constitute approval.

7. 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