



Securing Data at UTRGV

www.utrgv.edu/is
is@utrgv.edu

Dr. Kevin Crouse, DBA
Chief Information Security Officer

Topics to cover

Policy Review

Standards to protect

Protecting Data at Rest

Protecting Data in Transit

Approved Data Storage locations

Software/Technology Assessments

Some useful tools and technologies

Policy Reviews

TAC 202



- Establishes information Security Standards for Institutions of Higher Education.

UTS 165



- This policy establishes a comprehensive information security governance framework to manage information security risks, aligning them with the strategic goals of the UT System institutions.

UTRGV HOP & AUP



- HOP 09-101 Information Resources and Security Policy.
- Acceptable Use Policy for users and computers accessing UTRGV information resources as defined by UTS 165



Data protection standards

FERPA

Student
Records

HIPAA

Health
Records

PCI-
DSS

Credit Cards
Records

GDPR

European
Union
Privacy

CUI

Sensitive
Unclassified
Information

CMMC

Safeguarding
CUI and
Sensitive
Classified
Information



Types of University Data?



Restrictive /
Confidential

Internal /
Controlled

Public /
Published

How do we protect data?

Protect data in transit



Protect data at rest



Protecting data in transit

- UTRGV employs a multi-faceted approach to protect data in motion, emphasizing encryption and secure transmission methods.





Protecting data at rest?

- UTRGV protects data at rest by implementing encryption for confidential data stored on media and devices. Additionally, they require physical security measures for devices containing sensitive information and enforce access controls, including password protection for devices and encrypted, preferably immutable, backups.



Approved Data Storage Locations Restrictive / Confidential Data

Data Storage Locations for Restricted / Confidential Data					
Data Storage Service Location	FERPA	HIPAA	GLBA	SSN	Extended List
UTRGV Employee 365 E-mail	Yes	Yes ¹	No	No	Extended List Document Link
UTRGV Central IT 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	
Other non UTRGV Storage	Must follow the Security Exception Process.				
Non-central IT supported cloud storage	Must follow the Security Exception Process.				
Student personal device	Please reference Data Classification Standard for Students.				



Approved Data Storage Locations

Restrictive/Confidential Data Notes

- (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.



Approved Data Storage Locations Internal/Controlled Data

Data Storage Locations for Internal / Controlled Data	
Data Storage Service Location	Internal / Controlled Data
UTRGV Central IT 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



Approved Data Storage Locations Public/Published Data

Data Storage Locations for Public / Published Data	
Data Storage Service Location	UTRGV affiliates and public with a “need to know”.
UTRGV Employee 365 E-mail	Yes
UTRGV Central IT Storage	Yes
UTRGV Owned Server	Yes
UTRGV Researcher MS SharePoint, Teams & OneDrive	Yes
UTRGV Computer	Yes
UTRGV Mobile Phone	Yes
Personal Computer	Yes
UTRGV Owned NAS Storage	Yes
Other Storage	Must follow the Security Exception Process.

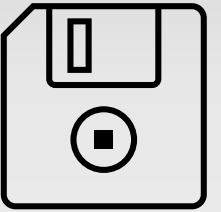




Data Retention and Disposal

All research records must be retained per the:

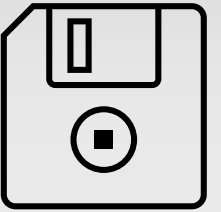
- UTRGV Records Retention Schedule
- Grant or contract funder requirements.
- Applicable research, IRB or other relevant requirements.
- [Data Retention and Disposal Policy](#)



Data Management Plan

Researchers are encouraged to develop Data Management Plans that include:

- Data classification and sensitivity
- Storage and backup strategies
- Access control and sharing protocols
- Retention and disposal procedures
- Security measures aligned with UTRGV and sponsor requirements
- Data Retention and Disposal Policy



Software / Technology Assessment

Get IT and Security Approval Before You



Tools and Technology

Encrypting UTRGV O365 Email

To further secure an email or to encrypt content to an external recipient:

Include **[secure]** tag at the beginning of the subject field of your email.

For Example:

Subject: **[secure]** Monthly Report





Tools and Technology

Liquid Files

What is Liquid Files?

Liquid files will be used for securely sharing protected information that cannot be shared by other means such as email attachments or online shares. Examples of protected information are documents containing FERPA information, HIPAA, and Social Security Numbers.

How do I access Liquid Files?

You can get access to the software to **send** and **request** files by accessing the application

URL <https://securetransfer.utrgv.edu>
and entering your UTRGV
credentials.



Location of documentation

ISO Website: [HTTPS://www.utrgv.edu/is](https://www.utrgv.edu/is)

- [Data Classification Standard for Faculty](#)
- [Data Classification Standard for Students](#)
- [Data Retention and Disposal Policy](#)
- [Software/Technology Assessment](#)



The University of Texas
Rio Grande ValleyTM
.....
Information Security Office



Securing Data at UTRGV

www.utrgv.edu/is
is@utrgv.edu

Dr. Kevin Crouse, DBA
Chief Information Security Officer