The University of Texas Rio Grande Valley
Information Security Office

UTRGV Research Data Retention and Disposal Policy

Table of Contents

Contents

UTRGV Research Data Retention and Disposal Policy

1. Purpose

This policy establishes guidelines for the retention, storage, and disposal of research data generated or acquired through activities at The University of Texas Rio Grande Valley (UTRGV).

The objectives are to:

- Ensure compliance with applicable federal and state laws, including the Texas Government Code, Chapter 441.
- Meet the requirements of sponsoring agencies (e.g., NIH, NSF).
- Protect intellectual property and support responsible dissemination of research.
- Maintain the integrity, confidentiality, and availability of research data for accountability, reproducibility, and future use.
- Enforce information security controls to mitigate risks of data breaches, unauthorized access, and data loss.

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 and Audience

- This policy applies to all individuals engaged in research under UTRGV's auspices, including faculty, staff, students, and affiliated personnel. It covers all research data and associated records, regardless of format (e.g., physical, electronic, biological).

4. Data Ownership and Stewardship

- Research data generated using UTRGV resources is the property of the university.
- UTRGV is responsible for ensuring data integrity, security, and retention.
- Data Stewards must manage data in accordance with:
    - UTRGV's Minimum Security Standards for Data Stewardship
    - UT System Information Security Standards (UTS165)
    - Applicable federal or state regulations including but not limited to the following:
        - Federal Information Security Modernization Act (FISMA)
        - Health Insurance Portability and Accountability Act (HIPAA)
        - Family Educational Rights and Privacy Act (FERPA)

5. Data Retention

1. Retention Schedule:

- All research records must be retained per the:
    - UTRGV Records Retention Schedule,
    - UTRGV Institutional Animal Care and Use Committee (IACUC, once approved)
    - UTRGV Institutional Bio Safety Committee (IBC, once approved).

2. Minimum Retention Period

- Research data must be retained for at least three years after project completion or submission of final reports for federally funded projects, unless otherwise specified.
- Before destroying data make sure to follow the appropriate records retention information disposal process.

3. Extended Retention Requirements

Retention periods may be extended due to:

- Grant Requirement: Specific condition set by the funding agencies or sponsors. These requirements often stipulate how long research data must be retained.
- Legal Hold: Data under audit, investigation, or litigation must be preserved until resolution.
- Intellectual Property: Retain data as long as necessary to protect IP rights.
- Clinical Research: Follow UTRGV DM-504 and related SOPs for clinical trials.
- Student/Trainee Involvement: Retain data until the student's graduation or departure.

- HIPAA: Data subject to HIPAA must be retained for at least six years post-project, per UT System HIPAA Policy 3.4.

6. Data Storage Access

A. Storage Location

- Data must be stored on UTRGV-approved systems or secure cloud services that meet institutional and regulatory security standards.
- Physical records may be transferred to UTRGV Records Management following proper procedures.

B. Security Requirements

All research data must be protected using the following controls:

- Access Control: Role-based access must be enforced. Only authorized personnel may access sensitive or protected data.
- Encryption: Sensitive data must be encrypted at rest and in transit using FIPS 140-2 compliant methods.
- Authentication: Multi-factor authentication (MFA) must be used for systems storing or processing sensitive research data.
- Backups: Regular, encrypted backups must be maintained and tested for recoverability.
- Monitoring: Systems must be monitored for unauthorized access or anomalies, in coordination with UTRGV's Information Security Office.
- Incident Response: Any suspected data breach must be reported immediately to the Information Security Office per the UTRGV Incident Response Plan.
- Controls required for the protection of research data must follow the guidelines established in UTS 165 and UTRGV standards, including control determination prior to project initiation.

C. Departing Faculty

Faculty leaving UTRGV must:

- Notify their Department Chair and the Office of Clinical Research (if applicable).
- Follow the PI Separation Checklist and Departing Investigator Policy.
- Obtain written approval from the **Department Chair** and **EVP/CAO** (or designee) to take copies or originals.
- Submit requests **at least 90 days** before departure, or within three days of notice that is less than 90 days prior to departure.
- Cover any costs associated with data transfer.
- If permitted to take original data, retain it per policy and provide UTRGV with a complete, accessible copy.
- Ensure continued compliance with data security requirements post-departure.

D. Departing Students

- Students leaving UTRGV who have participated in research projects must:
  - Notify the Principal Faculty Sponsor:
    Inform the Faculty Sponsor and, if applicable, the research supervisor of their departure and any research data in their possession.
  - Data Transfer and Access:
    Return all original research data, records, and materials to the Faculty Sponsor or designated Data Steward prior to departure. Students may request copies of data for personal use (e.g., for portfolios or future research), subject to written approval from the Faculty Sponsor and compliance with university policies and sponsor requirements.
  - Compliance:
    Ensure that any data retained or transferred complies with confidentiality, intellectual property, and data security requirements, including applicable federal and state regulations (e.g., HIPAA, FERPA).
  - Documentation:
    Complete any required separation checklists or forms as directed by the PI or department.
  - Data Security:
    Confirm that all electronic data is removed from personal devices and accounts, and that no unauthorized copies remain after departure.
  - Retention:
    Data associated with student research must be retained by UTRGV per the university's retention schedule, regardless of the student's status.

7. Data Management Plans (DMPs)

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 and ensure that all electronic media storing records is properly wiped, sanitized, or destroyed following UTRGV guidelines.
- Outline the plan to follow all UTRGV Security Requirements (see above).
- Security measures aligned with UTRGV and sponsor requirements

8. Revision History

Revision History			
Version	**Date**	**New**	**Original**
1.0	8/15/2025	Created document	Entire document has changed.

9. Sources

10. Approvals

Approvals		
Name	**Role**	**Date**
Kevin Crouse	CISO	8/15/2025
Kevin Crouse	CISO	10/20/2025