Applies to: *Faculty (including part-time and visiting faculty), staff and students (including graduate/undergraduate student workers and graduate assistants) employed by the University This policy continues to apply to individuals on sabbatical, other leaves or while visiting other institutions*

1. Policy:

Issued: June 2025
Last Revised:
Last Reviewed:

2. Policy Purpose:

This policy establishes requirements for the secure backup, storage, and recovery of university data managed by the IT department. It ensures data integrity, availability, and compliance with the Family Educational Rights and Privacy Act (FERPA).

3. Scope and Application:

This policy applies to:
- All on-premise servers and storage systems managed by Central IT.
- All cloud-based services (SaaS) used for university operations where Central IT is the administrator or data steward.

4. Definitions:

Definitions	
RTO	Recovery Time Objective
RPO	Recovery Point Objective

5. Policy Details:

5.1 General Principles

- All critical university data must be backed up regularly.
- Backups must be encrypted in transit and at rest.
- Backup and storage systems must be protected against unauthorized access.

- Data must be recoverable within a defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

5.2 On-Premise Systems

- Backup Frequency: Daily incremental and weekly full backups. See backup schedule.
- Retention: Minimum of 30 days for daily backups; 6 months for monthly snapshots.
- Storage Locations: Primary data center two geographically separate secondary site. One is in Adrienne hall and the second is in the cloud.
- Testing: Quarterly restore tests must be performed and documented.
- Encryption: AES-256 encryption must be used for all backup media.

5.3 Cloud/SaaS Services

- Vendor Responsibility: Ensure vendors provide adequate backup and disaster recovery capabilities.
- Data Export: Where possible, configure automated exports of critical data to university-controlled storage.
- Review: Annual review of vendor backup practices and compliance with FERPA.
- Third-Party Risk: All SaaS vendors must sign a Data Protection Agreement (DPA) and demonstrate FERPA compliance.
- Testing: Quarterly restore tests must be performed and documented.

5.4 FERPA Compliance

- Backups must not be stored in locations that allow unauthorized access to student education records.
- Access to backup data must be logged and monitored.
- Any data breach involving backup systems must be reported in accordance with the university's incident response plan procedures:

6. Responsibilities:

Position or Office	Responsibilities
Information Technology	Implements and maintains backup systems, performs regular testing, and ensures compliance.
Data Owners	Identify critical data and coordinate with IT for appropriate backup strategies.
Technical Director	Reviews encryption and access controls annually.

7. Related Information:

Related Policies
Information Security Policy
Data Governance Policy

8. Contacts:

Division/ Department	Position or Office	Contact Information
Information Technology	CIO	603-897-8630 / itsupport@rivier.edu