IT Backup Standard

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
11/20/2023	04/05/2024	Division of Information Technology IT Security Office

POLICY STATEMENT

It is the policy of Florida International University that all data pertaining to the institution must be systematically backed up. Scheduled restoration of data will be performed regularly to audit the backup process, ensuring its effectiveness and reliability. This proactive approach aligns with our commitment to maintaining the integrity, availability, and confidentiality of institutional data, thereby safeguarding the interests of our stakeholders and meeting the requirements imposed by regulatory bodies.

SCOPE

This policy applies to all institutional data within the institution's stewardship. It encompasses data stored on servers, databases, workstations, mobile devices, and any other medium containing institutional information.

REASON FOR POLICY

In today's dynamic and technologically driven environment, the importance of a comprehensive enterprise-wide data backup policy cannot be overstated. Safeguarding institutional data is paramount not only for operational continuity but also to comply with various regulations, standards, and laws governing data protection. Compliance with these mandates necessitates a structured and diligently executed data backup policy to mitigate risks associated with data loss, corruption, and unauthorized access.

DEFINITIONS

TERM	DEFINITIONS

Institutional Data	Any data generated, processed, or maintained by the institution, including but not limited to student records, financial information, research data, and administrative documents.
Scheduled Restoration	The planned process of recovering data from backups at predetermined intervals to verify the effectiveness of the backup system.
Data Loss	The unintended and irreversible loss of data, which may result from various factors such as hardware failure, software errors, or malicious activities.
Information System	The combination of hardware, software, data, personnel, procedures, and facilities organized to collect, process, store, and disseminate information within an institution.

ROLES AND RESPONSIBILITIES

Effective implementation of the data backup policy relies on the collaboration and accountability of various stakeholders within the institution. Each department and school is responsible for the creation, maintenance, execution, and testing of the backup system and strategy. The following roles and responsibilities are defined:

1. Department of IT (DoIT):
   - Develop and maintain the overall data backup system.
   - Execute and monitor scheduled backups.
   - Conduct regular testing of backups.

2. Department and School Administrators:
   - Collaborate on department-specific backup procedures.
   - Ensure integration of backup procedures into workflows.
   - Oversee day-to-day execution and testing at the departmental level.

3. End Users and Data Owners:
   - Adhere to backup policies.
   - Collaborate with IT for critical data inclusion.
   - Participate in testing exercises.

4. Institutional Compliance Officer:
   - Oversee compliance with backup policies.
   - Ensure alignment with regulations and standards.

5. Senior Management:
   - Provide support and resources for backup practices.
   - Emphasize the importance of data backup in risk management.

FLORIDA INTERNATIONAL UNIVERSITY

RELATED RESOURCES

https://security.fiu.edu

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 ST, PC534
Miami, FL 33199
Security@fiu.edu
305-348-1366
https://security.fiu.edu

HISTORY

Initial Effective Date: April 5, 2024
Review Dates (review performed, no updates): Review Performed
Revision Dates (updates made to document):