Redeemer's University, Ede

Digital Records Backup Protocol

Effective Date: *1st September, 2025*

1. Purpose

This protocol establishes structured and secure procedures for backing up digital records and data across Redeemer's University. It ensures business continuity, data integrity, and compliance with regulatory requirements such as the **Nigeria Data Protection Regulation (NDPR)**.

2. Scope

This protocol applies to:

- All digital records stored or processed by the university (academic, administrative, student, research, medical, and financial)
- All university-owned systems, cloud services, and authorized user devices
- All departments, units, and third-party service providers handling university data

3. Backup Objectives

- Protect institutional data from loss due to hardware failure, human error, cyberattacks, or disasters
- Enable rapid recovery of mission-critical systems and information
- Ensure data consistency and integrity across multiple platforms
- Support compliance with legal and policy requirements

4. Types of Data to be Backed Up

- **Core Administrative Systems:** Payroll, HR, finance, student records (e.g., ERP, LMS, MIS)
- **Academic Records:** Course materials, exam results, faculty publications
- **Research Data:** Approved project data and publications
- **Email and Communication Systems**
- **User Directories and Configurations**

- **Websites and Application Databases**

5. Backup Frequency

Data Category	Backup Frequency	Type
Critical systems (ERP, email, student records)	Daily	Full & Incremental
Departmental shared drives	Weekly	Differential
User desktop folders (staff/student profiles)	Weekly	Incremental
Research data (ongoing projects)	Weekly (or after major updates)	Full
Archived data	Monthly	Full
Cloud platforms	Auto-synced daily	Mirrored or real-time

6. Backup Storage Locations

- **Primary Backup Storage:** On-site servers with RAID configuration in a secured data centre
- **Secondary Backup Storage:** Encrypted external storage devices (offline, stored off-site)
- **Cloud Backup Repository:** Secure university-managed cloud (e.g., Microsoft Azure, Google Cloud) with versioning and auto-restore
- **Air-gapped Backups:** Immutable copies stored without network access for critical archives

7. Security Measures

- All backup data must be **encrypted (AES-256)** both at rest and in transit.
- Access to backups is **restricted to authorized ICT personnel** only.
- **Multi-factor authentication (MFA)** and role-based access control (RBAC) must be implemented.
- Antivirus and anti-malware tools must scan backup systems regularly.

8. Backup Testing and Verification

- Test restores must be conducted **quarterly** to verify data recovery procedures.
- Logs of backup operations must be **automatically generated and reviewed** weekly.
- Failed or incomplete backups must be flagged and investigated within **24 hours**.

9. Retention of Backups

- Daily backups: Retained for **7 days**
- Weekly backups: Retained for **1 month**
- Monthly backups: Retained for **1 year**
- Annual archives: Retained for **5–7 years** depending on data classification

(Refer to the **University Data Retention Schedule** for specifics.)

10. Roles and Responsibilities

Role	Responsibilities
Directorate of ICT	Implementation, monitoring, maintenance, and reporting on backup systems
System Administrators	Execute and document backup processes, test recoveries
Data Protection Officer (DPO)	Ensure compliance with data protection and NDPR requirements
Unit Heads/Deans	Identify critical data for backup within their domains
Third-party vendors	Ensure contractual compliance with university backup and security standards

11. Incident Response and Recovery

- In the event of data loss, cyberattack, or corruption:
    - Immediate notification must be made to the **ICT Directorate** and **DPO**.
    - The ICT Directorate shall initiate the **Disaster Recovery Plan**.
    - Restoration of affected systems must begin **within 4 hours** for critical systems.

12. Review and Updates

- This protocol shall be reviewed **annually** or in response to changes in technology, threats, or regulations.
- Revisions must be approved by the **ICT Governance Committee** and reported to Senate.