Policy Title	Data Management and Backup Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Infrastructure and System administration offices
Pertinent Dates	created 18.03.2022 revised updated approved

I. SCOPE OF POLICY

This Policy applies to **all systems and applications administrators.** This policy applies to **all University-related systems and applications with critical data**.

II. DEFINITIONS

Information
Information is generally defined as "processed data or knowledge or facts about someone or something" and "the communication or reception of knowledge or intelligence". It can exist in many different formats but it must have meaning in some context for its receiver. For the purpose of this policy, the term 'information' refers to information, records and data.

Information System: An individual or collection of computing and networking equipment and software used to perform a discrete business function. Examples include the Datacenter systems, Network Systems, LMS, SIS, the ERP, lab systems and associated PCs or the set of desktop computers used to perform general duties in any department.

III. POLICY STATEMENT

The purpose of this policy is to ensure system administrators are aware of the backup policy used to govern the backup procedures and process for different applications on different systems.

IV. RESPONSIBILITIES

Backup administrator is responsible for the following

- Maintain backup media.

- Storing the backup disks.
- Checking if the backup has been successfully completed at the needed frequency.
- Troubleshooting and managing backup failure.
- Maintaining the backup log.

V. POLICY STANDARDS AND PROCEDURES

- Each system/application should have ownership form signed by the owner and approved by the CIO.
- At least once a week all AIU critical systems and production data are fully backed up.
- Other less critical systems/applications are fully backed up once monthly.
- Backup of systems and data should take place at night away of the working hours.
- Appropriate backup methods (i.e., full, incremental, or differential) should be employed daily in accordance with the allotted backup window.
- Backup media must adhere to industry accepted backup technology standards, such as:
  - The media's read/write capacity shall be rapid enough to permit the backup to be completed during the allotted time (i.e., before the start of the next business day)
  - The media's capacity shall be large enough to hold the complete backup
  - The media should be readable after a minimum of 5 years in unattended storage.
  - Data compression algorithms may be used to minimize the volume of data on the backup medium. When compression is employed, the selected parameters and algorithms must be documented and observed during data restoration (decompression).
- Regular maintenance of the backup device is carried out to ensure it is kept in good working order.
- If a particular file or file system is corrupted or destroyed or in case of partial data corruption, only that file or file system (or set of files) needs to be restored upon formal request from system/application owner.
- If a major outage caused by a natural or manmade disaster occur, many or all of the files and file systems may need to be restored. Such major restorations requires proper timing and sequencing due to business priorities and file dependencies. This part is covered on the Disaster Recovery Plan for each application.

VI. FORMS/INSTRUCTIONS (if applicable)

- System/Application Ownership Form
- Backup Information Form
- Backup Report

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Information Governance Policy
Information Security Policy

VIV. CONTACT INFORMATION

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.