Policy Title	Audit Logging and Monitoring 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 University-related data** in any format including data created, stored, processed or transmitted by AIU personnel.

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.

Log Files
Records (mostly text files) that are created automatically during system operation and contain entries about the events that happened in a system. They are vital for systems troubleshooting and analysis. For example Web Servers automatically save usage and activity information such as the date, time, IP address, HTTP status, bytes sent, and bytes received

III. POLICY STATEMENT

The purpose of this policy is to establish the procedures and responsibilities for providing accurate and comprehensive application and system logs for AIU applications and systems in order to detect and react to inappropriate access to, or use of, information systems or data. Logs need to be protected stored and retained adequately.

IV. RESPONSIBILITIES

V. POLICY STANDARDS AND PROCEDURES

Log files created by AIU systems and digital services should be kept and stored. All AIU systems and digital services should be configured to enable the proper level of logging details that is accepted to meet business, compliance, troubleshooting, information security needs

IT personnel are considered data custodians, hence they are responsible for enabling and keeping the logs existing and authentic as well as any business user who has the ability to deal with logs

ACCESS TO LOG FILES

While the usage logs covered under this policy do not contain personally identifying information, the logs are classified by AIU as confidential data. The reason for this is that the log files used in conjunction with other information that central IT has in its custody may allow us to associate specific information on the use of a service, such as specific Web page access, with a given individual's computer.

AIU will comply with a court order or valid subpoena that requests the disclosure of information contained in usage logs.

Information Security office is responsible for conducting Information security investigation and digital forensics activities with regards to any AIU's digital nature subjects. Also, the office is responsible for collecting and validating any digital information/logs and act as a central point of contact with any investigation parties whether internally or externally. Accordingly, Information Security office has the right to request data, meta data and technical logs and history input from AIU system's owners and administrators within the investigation's scope and through a documented communication.

RETENTION OF LOG FILES

Log file retention times are specified in the Retention Guidelines for Log Files. If a log file contains relevant information that is useful for future reference, a pending transaction, or as evidence of a management decision, it should be retained. If a log file is needed for these purposes, it is the responsibility of IT staff to move these specific logs to another central IT-owned system prior to the destruction of the log (even after it has reached its maximum retention time).

DESTRUCTION OF LOG FILES

Log files must be destroyed in accordance with the Retention Guidelines for Log Files. All original, backups, and copies of logs should be destroyed. For this reason, log files should not be backed up to removable media and should stay on the centralized log server or the local file system of the machine on which they are generated. In addition, care should be taken to exclude log files from computer disk images. This policy recommends deleting log files as opposed to log entries. Logs should be destroyed in the most destructive and economical way available. Actual deletion method should be specified in the Retention Guidelines for Log Files as it depends on the type and class of data.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

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.