Policy Title	Information Governance Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	CIO Office
Pertinent Dates	created 18.03.2022 revised updated approved

I. SCOPE OF POLICY

This Policy applies to **all staff employed by or affiliated** (temporary or permanently) with the University, including staff, students, contractors, hourly paid staff and visitors.

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.

Documents
ISO9000 defines a document as "information and its supporting medium", so it can include a wide range of both hard copy and digital formats, and is not simply limited to written information.
Documents can be created in many formats, including (but not limited to):

- Letters (digital and hard copy)
- Emails and official communications
- Policies and guidance
- Meeting papers and minutes
- Reports
- Contracts
- Presentations

III. POLICY STATEMENT

The purpose of this policy is to establish the key principles of Information Governance at AIU and set out responsibilities and reporting lines for members of staff to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximize operational efficiency.

IV. RESPONSIBILITIES

- Information governance is overseen by the Chief Information Officer (CIO).
- The **Information Trustees** are senior University officials (typically at the level of Vice President or higher) who have planning and policy-making responsibilities for University Information and for the establishment of operational processes to collect and record data in accordance with University business rules. The Information Trustees, as a group, are responsible for overseeing the establishment of information management policies and procedures, and for the assignment of information management accountability.
- **Information Domain Trustees** are senior managers in operational areas responsible for maintaining the content of Transactional Systems. They implement policy as established by Information Trustees, assign Information Stewards, and serve as the first escalation point for problem/policy resolution from the Information Stewards.
- **Information Stewards** are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the Transactional Systems. Information Stewards are appointed by the respective Information Domain Trustees
- **Information Custodian** are **all AIU staff employed by or affiliated** (temporary or permanently) with the University, including staff, students, contractors, hourly paid staff and visitors and third parties are responsible for:
    - ensuring the quality and completeness of information which they collect or create
    - ensuring that they understand and adhere to procedures and resources under this policy and related policies which govern the management, control, storage, transfer and destruction of information throughout its lifecycle
    - supporting a culture that promotes good information governance practices and reporting any identified compliance breaches or incidents
    - managing AIU information in accordance with the Privacy Policy and Information Technology and Security Policy.
- Data Users are individuals who receive authorization from the **Information** Steward to access, enter, or update information. Data Users must use the resource only for the purpose specified by the Data Steward, complying with controls established by the Steward, and preventing disclosure or confidential or protected information.

V. POLICY STANDARDS AND PROCEDURES

This policy is to be augmented with the following standards and procedures
Refer to the following documents which are established in accordance with this policy:

- Data Classification Standard
- Destruction of Information Procedure

This policy is to be read in conjunction with

- Research Policies
- Data Management and Backup Policy
- Audit Logging and Monitoring Policy

- Information Security Policy

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

VIV. CONTACT INFORMATION

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