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

I. SCOPE OF POLICY

The purpose of this policy is to establish a process to manage risks to AIU that result from threats to the confidentiality, integrity and availability of university data and information systems.
This policy applies to all electronic data created, stored, processed or transmitted by the AIU, and the information systems used with that data.
This policy applies globally to all assets, information resources and related infrastructure owned, managed or administered by AIU or owned and operated by a third party on behalf of AIU.
Also, this policy applies to anyone with access to AIU's information and information technology assets, including permanent, temporary or contracted employees, consultants, volunteers or third-party organizations

II. DEFINITIONS

Risk - A risk is commonly defined as an effect of uncertainty on the achievement of objectives. In other words, risks are various events that can affect the achievement of objectives. Risk can have both negative and positive outcomes. Our aim is to manage the adverse effects and turn the risk into value.
Risk management - All activities performed by AIU to anticipate, identify, assess and control the uncertainties which may impact on AIU's ability to achieve its aims, objectives and opportunities. These will range from university-wide to specific projects or programs, to the individual members.

III. POLICY STATEMENT

- All information systems must be assessed for risk to AIU that results from threats to the integrity, availability and confidentiality of AIU data. Assessments should be completed prior to purchase of, or significant changes to, an information system; and at least every 2 years for systems that store, process or transmit restricted data.
- Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.

- Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by the Chief Privacy Officer and Chief Information Security Officer. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.
- Each information system must have a system security plan, prepared using input from risk, security and vulnerability assessments.

IV. RESPONSIBILITIES

- Information Security Administrators (ISAs) are responsible for ensuring that their unit conducts risk assessments on Information Systems, and uses the university approved process.
- Information Security Engineers are responsible for assessing and mitigating risks using the university approved process.
- Information System Owners (ISOs) are responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred or accepted.
- The Chief Information Officer (CIO) is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

V. POLICY STANDARDS AND PROCEDURES

Risk Assessment Standard:

- Risk assessments will be conducted:
  - Prior to acquisition of information systems.
  - When an existing information system undergoes a significant change in technology or use that would affect its risk posture. Examples include significant software upgrades, changes in hosting platforms or vendors, or changes in the data classification or volume of records stored, processed or transmitted by the system.
  - At least every two years for systems that store, process or transmit restricted data and three years for all other systems.
- The approved university risk assessment process will include the following:
  - The scope of the assessment.
  - An assessment of security control implementation.
  - Report documenting threats, vulnerabilities and risks associated with the information system.
  - Recommendations to increase the security posture of the information system.
- The Information Security Office will retain risk assessment records according to the university records retention schedules and applicable laws.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Incident Response Policy

VIV. CONTACT INFORMATION

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