AUM
AMERICAN UNIVERSITY OF MALTA

Policy: **IT RISK MANAGEMENT POLICY**

Policy Title	**IT RISK MANAGEMENT POLICY**
Policy Ref:	AUM-2024_IT_Risk_Mngt_V2
Effective Date	June 2024
Responsible Office	Provost Office
Responsible Executive(s)	IT Department

Purpose

To establish a process to manage risks to the University of AUM that result from threats to the confidentiality, integrity and availability of University Data and Information Systems.

Scope

This policy applies to all electronic data created, stored, processed or transmitted by the American University of Malta, and the Information Systems used with that data.

Principles of Data Risks

This policy helps to protect AUM from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Policy

- All Information Systems must be assessed for risk to the AUM that results from threats to the integrity, availability and confidentiality of AUM 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 Information Technology Department. 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.

Responsibilities

1. The Information Technology Department is responsible for ensuring that their unit conducts risk assessments on Information Systems and uses the university approved process.
2. Information Technology Department and Management is responsible for assessing and mitigating risks using the university approved process.