Policy Title	Securing Technology Resources and Services
Responsible AIU Office **(Higher Management/Directorate)**	Chief Information Officer (CIO)
Policy Owner **(Executive Department/Office)**	Institutional Information Systems Unit Website and Portal Unit IT Infrastructure and Data Center Unit IT Security Office (ISO)
Pertinent Dates	July 2022

I. SCOPE OF POLICY

This Policy provides direction and establishes requirements for controlling and managing access to IT Resources, Services and equipment of AIU and its' affiliates to prevent unauthorized physical access, damage, and interference to information assets.

Information technology resources and services are critical resources essential to the mission and business of the university.
Every facet of the enterprise is affected by the resources attached to the network.
Outages of the network or information services will adversely affect the daily operations and functions of the university.
This policy ensures that all technology resources and services are as stable, secure and trustworthy as possible.

This policy applies to any technology resource or service that:

- Is owned or managed by the university;
- Is connected to the university network;
- Connects to another university technology resource or service; or
- Stores university data or information.

This policy applies whether the network connections are remote or campus-based.
The owner of a technology resource may use it at his or her discretion; however, once a device is connected to the university network; or other technology resource or service is used to store university data; it is subject to applicable laws and regulations and to university policies.

II. DEFINITIONS

Technology resource – any item such as a computer, tablet, smartphone, or similar device and associated peripherals owned by AIU or used to store university data, including those in research contracts or private activities associated with the university, and privately-owned technology devices that are connected to the AIU network or used to store university data.

Service – a set of computer and network applications that perform work, often operating on data using standard protocols.

III. POLICY STATEMENT

Information technology resources and services must be securely maintained in compliance with the regulations, policies and standards contained herein and information published on University website or communicated through the official email, and must be associated with an individual who is responsible for ensuring their continued security.

ISO must identify security mechanisms, service levels and management requirements of all network services and include them in network services agreements, whether these services are provided in-house or outsourced.

ISO with the help of Engineering Services must implement safety measures to protect against unauthorized or unlawful physical access and/or theft of IT equipment and define and use appropriate security perimeters to protect areas that contain either sensitive or critical information assets. All fire doors on a security perimeter must be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; Implementing safety measures to protect IT equipment against environmental hazards.

IV. RESPONSIBILITIES

The Chief Information Officer (CIO) is responsible for creating and maintaining information technology (IT) related security policies and standards across the university and is assigned the authority for ensuring compliance with those standards. IT-related policies and standards are posted on the University website.

The IT Security Office (ISO) will ensure that security training and security tools are available and that security standards are published and updated.

Every technology resource user is responsible for security and acceptable use of the material he or she chooses to access, store, print, send, display or share with others.

University departments and organizations are responsible for assigning each technology resource to an accountable individual who is responsible for ensuring the continued security of that resource as required by Division of IT policies and standards.

Individuals – including individual students – using personal technology resources are responsible for complying with the university's Minimum Security Standards.

University departments must regularly analyze risks for their technology assets using the AIU Risk Assessment process.

Formatted: Font: Complex Script Font: Times New Roman, 11 pt

V. POLICY STANDARDS AND PROCEDURES

Departments and individual users must take actions to minimize security vulnerabilities that may exist on departmental and individual technology resources that they attach to a university network.

Training and consultation is available by contacting the IT Security Office.

Every technology resource user is subject to applicable laws and regulations and to university policies.

Enforcement:
Sanctions for violations may be determined by these laws and regulations in addition to and independently of any actions taken by the university.
Violators are subject to disciplinary action as prescribed in the Honor Codes, the Student Code of Conduct, and Human Resources policies and procedures. Violations of this policy are considered serious
and consequences for a specific violation may include the following:

- Any technology resource that is determined by the university to not meet the security standards may be refused connection to the university network.
- Network traffic to and from any device determined to be using the network inappropriately or in violation of the Acceptable Use Policy (Policy 7000) may be monitored. The university reserves the right to disconnect any resource from the network until suspected security incidents can be resolved. Attempts to notify the responsible person will be made before any such termination of network access.
- In cases where university network resources and privileges are threatened by improperly maintained devices (university owned or privately owned), the IT Security Office will offer mitigation strategies and, when necessary, act to eliminate the threat.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Information Security Policy

VIV. CONTACT INFORMATION

Chief Information Officer (CIO)

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

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