Policy Title	Acceptable Use of Technology Resources Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Information Technology (IT) Department - Information Security Office (ISO)
Pertinent Dates	July 2022.

I. SCOPE OF POLICY

This Acceptable Use of Information Technology Resources Policy (Policy) establishes requirements for the use and management of Alamein International University's Information Technology Resources to ensure their Confidentiality, Integrity, and Availability supports Alamein International University's educational, research, outreach, and administrative objectives.

The purpose is to provide rules for the appropriate use of all information technology resources, services, Internet, general use of hardware and software, system access, and other areas related to the security of systems and data.

This policy applies globally to anyone with access to AIU information and information technology assets, including permanent, temporary or contracted employees, consultants, volunteers or third-party organizations (henceforth referred to as the "users") irrespective of the time of day, means of access, or location of the person.

II. DEFINITIONS

- Availability (of Information Technology Resources): Ensuring timely and reliable access to and use of information.
- Authentication Method: Hardware or software-based mechanisms that force users to prove their identity before accessing data on a device. Example in use at Alamein International University includes but not limited to AIU Portal (Students' services portal).
- Confidentiality (of Information Technology Resources): Ensuring Electronic Information and Information Technology Resources are protected from unauthorized access.
- Desktop, Laptop, Mobile, or Other Endpoint Device: Any device, regardless of ownership, that has been used to store, access, or transmit Electronic Information, not classified as a Server. These devices are intended to be accessed directly by individuals and include, but are not limited to desktops, laptops, mobile phones, and tablets.

- Electronic Information: Often referred to as Electronically Stored Information (ESI). Any documents or information stored, in electronic form, on or sourced from Information Technology Resources. Common examples include: documents, spreadsheets, digital photographs, videos, communications (emails and their attachments, instant messages), voicemails, logs, data stored in Alamein International University funded or contracted cloud services, and data stored on Alamein International University Owned devices, including, but not limited to: laptops, desktops, cell phones, and Servers.

- Information Technology Resources: Alamein International University owned facilities, technologies, and information resources used for Alamein International University processing, transfer, storage, and communications. Included, without limitations, in this definition are computer labs, classroom technologies, computing and electronic devices and services, email, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all inclusive but rather reflects examples of equipment, supplies and services. This also includes services that are Alamein International University owned, leased, operated or provided by Alamein International University or otherwise connected to Alamein International University resources, such as cloud and Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or any other connected/hosted service.

- Integrity (of Information Technology Resources): Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

- Server: A computer program or device that provides dedicated functionality to clients. These are normally managed by professional information technology practitioners.

- Two-Step Authentication: A method to protect an account or system that requires more than one means to access it, such as providing a password as well as a response to a verification code sent to a physical device.

III. POLICY STATEMENT

- Users of Information Technology Resources are responsible for the content of their individual communications and may be subject to personal liability resulting from that use. Alamein International University accepts no responsibility or liability for any individual or unauthorized use of Information Technology Resources by users.

- Access to Information Technology Resources is a privilege and continued access is contingent upon compliance with this and other Alamein International University policies.

IV. RESPONSIBILITIES

- All individuals to whom this Policy applies are responsible for becoming familiar with and following this Policy. Alamein International University supervisors are responsible for promoting the understanding of this Policy and for taking appropriate steps to help ensure compliance with it.

- Users responsibilities:

- Review, understand, and comply with policies, laws, and contractual obligations related to access, acceptable use, and security of Information Technology Resources.
- Consult with the Information Technology (IT) department - Information Security Office (ISO) on acceptable use issues not specifically addressed in this Policy.
- Protect personal information and personal assets used to access Electronic Information.
- Use only authorized Information Technology Resources and only in the manner and to the extent authorized.
- Follow the user specific security controls in Minimum Security Standards for Desktop, Laptop, Mobile, and Other Endpoint Devices on personal assets, including, but not limited to, encryption, installing updates, virus protection, and Two-Step Authentication.
- Report the loss or theft of any Desktop, Laptop, Mobile, or Other Endpoint Device containing Electronic Information to the Information Security Office (ISO).
- Report any breach or suspected breach of a Desktop, Laptop, Mobile, or Other Endpoint Device containing Electronic Information to Information Security Office (ISO)
- Report suspected violations of this Policy to Information Security Office (ISO).

- Administrators responsibilities:
- Work with Information Security Office (ISO) to investigate alleged violations of this Policy; and Report suspected violations of this Policy to Information Security Office (ISO).

- Information Technology Professionals:
- Follow specific security controls in Minimum Security Standards for Servers and Minimum-Security Standards for Desktop, Laptop, Mobile, and Other Endpoint Devices on Alamein International University managed resources.
- Respond to questions from users related to appropriate use of Information Technology Resources.
- Work with Information Security Office (ISO) to investigate alleged violations of this Policy.
- Report the loss or theft of any Server containing Electronic Information to the Information Security Office (ISO).
- Report any breach or suspected breach of a Server containing Electronic Information to Information Security Office (ISO) and Report suspected violations of this Policy to Information Security Office (ISO).

- Chief Information Security Officer:
- Delegate authority and responsibility for investigating alleged violations of this Policy.
- Designate individuals who have the responsibility and authority to refer violations to appropriate Alamein International University offices for resolution or disciplinary action.
- Designate individuals who have the responsibility and authority to employ security measures and ensure that appropriate and timely action is taken on acceptable use violations.

- Chief Digital Information Officer:
- Designate individuals who have the responsibility and authority for Information Technology Resources.
- Designate individuals who have the responsibility and authority for establishing policies for access to and acceptable use of Information Technology Resources.
- Designate individuals who have the responsibility and authority for monitoring and managing system resource usage.
- Designate individuals who have the responsibility and authority for investigating alleged violations of this Policy.

- Office of Information Security Office (ISO):
  - Investigate suspected violations of this Policy.
  - Refer alleged violations to appropriate Alamein International University offices for resolution or disciplinary action.
  - Ensure that appropriate and timely action is taken on alleged violations.
  - Coordinate with appropriate Internet Service Providers and law enforcement entities on violations of this Policy.

V. POLICY STANDARDS AND PROCEDURES

- Use of Information Technology Resources:
  - Must adhere to the Alamein International University Code of Conduct and the Code of Student Conduct.
  - Must be consistent with the educational mission, research goals, outreach, and administrative objectives of Alamein International University.
  - Must adhere to applicable laws, regulations, Alamein International University policies, contractual agreements, and licensing agreements.
  - Must avoid actions that jeopardize the Confidentiality, Availability, and Integrity of the resources.
  - Must respect the rights of all users.
  - Must be consistent with the user's role or relationship to Alamein International University and used only in a manner and to the extent authorized by Alamein International University.

- Unacceptable Use

  Users of Information Technology Resources must NOT:
  - Violate any Alamein International University policies or rules.
  - Use Information Technology Resources for unethical, illegal, or criminal purposes.
  - Use Information Technology Resources for commercial purposes, except when explicitly approved by an authorized Alamein International University official.
  - Use Information Technology Resources for personal economic gain.
  - Violate the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws and regulations.
  - Copy, distribute, or transmit unauthorized copyrighted materials.
  - Use Information Technology Resources in a libelous, slanderous, or harassing manner.
  - Violate the privacy of co-workers, students, research subjects, alumni(ae).
  - Consume excessive Information Technology Resources.
  - Engage in any unauthorized circumvention, attempted circumvention, or assist another in circumventing security controls protecting Information Technology Resources.
  - Engage in any unauthorized activity that intentionally impacts the Integrity of Information Technology Resources or any resources external to Alamein International University that could result in a disruption, destruction, or corruption of Information Technology Resources.
  - Use credentials for which they are not explicitly authorized, attempt to capture, or guess credentials, in any way attempt to gain access to an unauthorized account.
  - Share personal password(s) with others or enable unauthorized users to access Information Technology Resources, or otherwise violate the Network Connection Policy.

- Create any program, web form, or other mechanism that authenticates with Alamein International University credentials, unless the Authentication Method is authorized by Office of Information Technology.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

- Personal Credentials Creation and Management Policy
- Email Communication Policy
- Access Control Policy
- Remote Access Management Policy
- Internet Use Policy
- University Network Use Policy

VIV. CONTACT INFORMATION

- Office of Information Technology (OIT) oit@aiu.edu.eg
- Information Security Office (ISO) iso@aiu.edu.eg

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