Policy Title	University Network Use Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Information Technology Department – Network Department Information Security Office (ISO)
Pertinent Dates	Created 12-03-2022

I. SCOPE OF POLICY

This policy is designed to protect the campus network and the ability of members of the Alamein International University community to use it. The purpose of this policy is to define the standards for connecting computers, servers or other devices to the University's network. The standards are designed to minimize the potential exposure to Alamein International University and its community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

Alamein International University must provide a secure network for its educational, research, instructional and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the university's campus network, thereby affecting many computers, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical Alamein International University internal systems. Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the Alamein International University network must follow specific standards and take specific actions.

This policy applies to all members of the Alamein International University community or visitors who have any device connected to the Alamein International University's network, including, but not limited to, desktop computers, laptops, servers, wireless computers, mobile devices, smartphones, specialized equipment, cameras, environmental control systems, and telephone system components. The policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to university-owned computers, personally-owned or leased computers that connect to the Alamein International University's network.

II. DEFINITIONS

III. POLICY STATEMENT

- Appropriate Connection Methods

A user may connect devices to the campus network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. As a result, extending or modifying Alamein International University's network is prohibited unless authorized by responsible Alamein International University's department.

- Network Registration

Users of the university network may be required to authenticate when connecting a device to it. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined below.

ISO maintains a database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary. For example, ISO would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person.

IV. RESPONSIBILITIES

- Responsibility for Security

Every computer or other device connected to the network, including a desktop computer has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in her office). For the sake of this policy, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to the Departmental Computing Coordinator or the Departmental Systems Administrator. Therefore, it is possible that one owner manages multiple departmental machines plus his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

V. POLICY STANDARDS AND PROCEDURES

- Security Standards

These security standards apply to all devices that connect to Alamein International University's network through standard university ports, through wireless services, and through home and off campus connections.

- Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week
- Computer owners must install the most recent security patches on the system as soon as practical or as directed by Information Security. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- Computer owners of computers that contain Alamein International University's Restricted Information should apply extra protections. ISO's Information Security Office will provide consultations on request to computer owners who would like more information on further security measures.

- Centrally-Provided Network-Based Services

ISO, the central computing organization, is responsible for providing reliable network services for the entire campus. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions will be made by ISO for approved personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server which requests from an individual their ISO-maintained password.

- Protection of the Network

ISO uses multiple methods to protect Alamein International University's network:

- monitoring for external intruders
- scanning hosts on the network for suspicious anomalies
- blocking harmful traffic

All network traffic passing in or out of Alamein International University's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, you are acknowledging that the network traffic to and from your computer may be scanned.

ISO routinely scans the Alamein International University's network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, you agree to have your computer or device scanned for possible vulnerabilities.

ISO reserves the right to take necessary steps to contain security exposures to the University and or improper network traffic. ISO will take action to contain devices that exhibit the behaviors indicated below, and allow normal traffic and central services to resume.

- imposing an exceptional load on a campus service
- exhibiting a pattern of network traffic that disrupts centrally provided services
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others
- exhibiting behavior consistent with host compromise

ISO reserves the right to restrict certain types of traffic coming into and across the Alamein International University's network. ISO restricts traffic that is known to cause damage to the network or hosts on it, such as NETBIOS. ISO also may control other types of traffic that consume too much network capacity, such as file-sharing traffic.

By connecting to the network, a user acknowledges that a computer or device that exhibits any of the behaviors listed above is in violation of this policy and will be removed from the network until it meets compliancy standards.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

- Acceptable Use of Technology Resources Policy
- Personal Credentials Creation and Management Policy
- Email Communication Policy
- Access Control Policy
- Remote Access Management Policy
- Internet Use Policy

VIV. CONTACT INFORMATION

- Center for Internet Security (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.