

Policy Title	Email Communication Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	Information Security Office (ISO)
Pertinent Dates	July 2022

I. SCOPE OF POLICY

Alamein International University's email services support the educational and administrative activities of the University and serve as a mean of official communication by and between users and Alamein International University. The purpose of this policy is to ensure that this critical service remains available, reliable, and is used for purposes appropriate to the University's mission.

This policy applies to all members of the Alamein International University community who are entitled to email services.

II. DEFINITIONS

N/A

III. POLICY STATEMENT

Alamein International University provides electronic mail (email) services to faculty, staff and students, and to other affiliated classes of individuals, including alumni and official visitors. Use of Alamein International University email services must be consistent with Alamein International University's educational goals and comply with applicable laws and university policies.

IV. RESPONSIBILITIES

- Faculty and Staff (full-time and part-time)

Email services are available for university faculty and staff to conduct and communicate University business. Incidental personal use of email is allowed with the understanding that the primary use be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

Email services are provided only while a user is employed by the University and once a user's electronic services are terminated, employees may no longer access the contents of their mailboxes, nor should they export their mailbox to a personal account before departure.

Faculty and Staff email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed by authorized University officials for purposes related to university business. Alamein International University has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

- Students

Email services are available for students to support learning and for communication by and between the University and themselves. The services are provided only while a student is enrolled in the University and once a student's electronic services are terminated, students may no longer access the contents of their mailboxes.

Student email users are advised that electronic data (and communications using the University network for transmission or storage) may be reviewed and/or accessed in accordance Alamein International University 's Acceptable Use Policy. Alamein International University has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

- Alumni and Others

Individuals with special relationships with Alamein International University, such as alumni or official visitors, who are neither employed nor enrolled at Alamein International University, may be granted limited email privileges, including an email address, commensurate with the nature of their special relationship. Alamein International University is free to discontinue these privileges at any time.

V. POLICY STANDARDS AND PROCEDURES

- **Acceptable Use under University Policies**

Email users have a responsibility to learn about and comply with Alamein International University's policies on acceptable uses of electronic services. Violation of Alamein International University policies (including this one) may result in disciplinary action dependent upon the nature of the violation.

Examples of prohibited uses of email include:

- Intentional and unauthorized access to other people's email.
- Sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail.
- Use of email for commercial activities or personal gain (except as specifically authorized by University policy and in accord with University procedures).
- Use of email for partisan political or lobbying activities.
- Sending of messages that constitute violations of Alamein International University's Code of Conduct.
- Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications.
- Use of email to transmit materials in a manner which violates copyright laws.

- Abuses of Alamein International University's email services should be directed to the Information Security Office at ISO@aiu.edu.eg

- **Security and Privacy of Email**

Alamein International University attempts to provide secure, private and reliable email services by following sound information technology practices. Since email services are provided through Microsoft services, Alamein International University cannot guarantee the security, privacy or reliability of its email service. All email users, therefore, should exercise extreme caution in using Alamein International University's email to communicate confidential or sensitive matters.

- Best Practices in Use of Email

- Confidential Information

When sending Alamein International University Restricted Information, the user must encrypt the message in an approved method.

- Malware

Alamein International University email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code, that can also install malicious programs on the workstation.

- Identity Theft

Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.

- Password Protection

Alamein International University's policy requires the use of strong passwords for the protection of email. A strong password must contain digits or punctuation characters as well as letters. In addition, your email password should be different from your Alamein International University network password.

- Departmental Email Boxes

Departments that provide services in response to email requests should create a shared mailbox to help support departmental functional continuity for managing requests sent via email.

- Forwarding Email

Alamein International University email users may choose to have their email delivered to a mailbox or forwarded to another mail repository. However, a non-Alamein International University forwarding address should not be used if there is a reasonable expectation that confidential information will be exchanged. Email is not considered a secure mechanism and should not be used to send information that is not considered public.

Staff email users on an extended absence should create an Out of Office message, which should include the contact information for another staff member who can respond while the user is away from the office.

- Compromised Accounts

An email account that has been compromised, whether through password-cracking, social engineering or any other means, must be promptly remedied with the appropriate means. The appropriate means will include a password reset, review of account settings, computer scans and malware disinfection to prevent possible leakage of personally identifiable information, spamming, potentially infecting others and degradations of network service. If the account is being used to harm others at Alamein International University and the owner cannot be reached in a reasonable period of time ("reasonable" being driven by the negative impact to the Alamein International University community), the Director of Information Technology Security will direct the Information Security Office (ISO) to reset the

password. Should the same account be compromised three or more times in any 12-month period, the account will be immediately suspended, and will not be re-enabled until the user notifies the Director of Information Technology Security to ensure that all remediation has taken place and is provided with remedial training.

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
- Access Control Policy
- Remote Access Management Policy
- Internet Use Policy
- University Network Use Policy

VIV. CONTACT INFORMATION

- 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.