October 2022

Document title: **[ELECTRONIC MAIL (Email) POLICY – Oct. 2022]**

Approval date: **[August 2017]**

Purpose of document: **[The Email policy governs usage of the University's Email system]**

Office/department responsible: **[Official of Information Security]**
Approved by: **[Nagwa Nicola, Chief Technology Officer]**

Document classification level: **[PUBLIC]**

Document accessible: **[https://www.aucegypt.edu/about/university-policies]**

Document includes: **[Policy]**

Related documents/see also: **[Information Security Policy, Acceptable Usage Policy]**

ELECTRONIC MAIL (Email) POLICY

Policy Statement

The American University in Cairo (AUC) provides its community with different electronic communication tools, including the Email system. The Email system supports the educational, research, and administrative activities of the University. It conducts a means of official communication among the members of AUC community and the external world.

AUC strongly encourages its community to use electronic mail to support its activities and promotes best practice guidelines to make that usage efficient and professional.

The Email policy governs the usage of the University's Email system.

Reason for Policy/Purpose

- To prevent unauthorized or inadvertent disclosure of sensitive AUC information
- To regulate Email usage for AUC's benefit
- To prevent tarnishing the public image of AUC
- To protect the university's legal position

- To provide confidentiality of communications, protection of privacy, and compliance with other university policies.

Who Approved This Policy

Nagwa Nicola, Chief Technology Officer

Who Needs to Know This Policy

This Email policy and rules apply to all members of the AUC community who are entitled to Email services. These include but are not limited to full-time or part-time faculty or staff, students, admins, alumni, independent contractors, interns, consultants, suppliers, clients, and other third parties.

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher, Chief Information Security, and Risk Officer
Responsible University Office: Office of Information Security

If you have any questions on the policy, you may send an email to infosec@aucegypt.edu

Definitions

Term (alphabetical order)	Definition as it relates to this policy
Chain Email	Email sent to successive people. Typically, the body of the message attempts to convince the recipient to make a number of copies of the message and pass them on to as many recipients as possible. It might promise the recipient of good luck and/or money or threaten him with bad luck and/or physical violence.
Credentials	Username and Password plus any other type of authentication if exist
Email	Electronic Mail - A method of exchanging digital messages from a sender to one or more recipients.
Forwarded Email	To resend an Email you received to other recipients
Sensitive information	Any Information is considered sensitive if it can affect AUC's business and reputation if disclosed

Policy/Procedures

General

1. Using the AUC Email account acknowledges the user's knowledge and acceptance of this policy and other AUC policies
2. The sender's identity, whether institutional or individual, must be clearly identifiable in all transmitted messages.
3. Email users have the responsibility to secure their Email credentials and to change them immediately if they suspect any disclosure
4. Emails accounts credentials can't be shared or used by different persons at any time
5. Mass mailing to the AUC community is only allowed through the University's administrator's approval
6. AUC Email service usage is governed under AUC Acceptable usage policy and other related AUC policies
7. Email messages & other related contents that are stored, created, and sent from AUC Email service are the property of the university. AUC reserve the right to monitor all emails transmitted for security and compliance.

8. The Information Security Office highly recommends that any information users consider sensitive or vulnerable be encrypted in order to add an extra layer of security
9. AUC has the authority to access and inspect the contents of any AUC email on a temporary or permanent basis; the access process is governed by AUC president's approval.
10. The creation and termination of AUC email accounts are governed through the "Email Creation and Termination Rules & Procedures "document.
11. AUC has the right to suspend, disable or terminate any AUC Email account on a temporary or permanent basis according to the management decision, end of the Email user relationship with AUC, or according to security risks or violation that are related to this account.
12. The Email service is an official way of communication in AUC, so all AUC Email users need to check their email on a frequent and consistent basis in recognition that certain communications may be time-critical.
13. Departmental accounts & credentials can't be used for other purposes other than sending and receiving emails.
14. Any AUC community member who both works and studies or had studied at AUC must have two separate AUC Email accounts, one for business and another one as a student or an Alumni.

Email Usage Scope for Staff, Faculty & Consultants

1. Email usage is restricted to AUC business correspondence and must be consistent with the relationship the individual has with the University.
2. Incidental personal usage is allowed putting into consideration that AUC is not responsible for personal emails storage, preservation, or extraction.
3. Email users shouldn't forward business Emails to any personal account, Email account's setting should be adjusted to keep copies in the AUC Inbox even if the user is using the email client option (Like Outlook)

Security & Privacy of Email

AUC will employ its best efforts to provide secure, private, and reliable Email services by following sound information technology practices. However, AUC cannot fully guarantee the security, privacy, or reliability of the Email service, putting into consideration that the Email service depends on third-party service providers. All Email users, therefore, should exercise extreme caution in using AUC Email to communicate confidential or sensitive matters.

Prohibited Use: The AUC's Email system should not be used for the creation or distribution of any disruptive or offensive messages: including but not limited to offensive comments about race, gender, hair, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

Email must not be sent in such a way as to harass others. Email users must not engage in frivolous, disturbing, or otherwise inconsiderate use or conduct in violations of the University's status as an independent, non-profit, apolitical, non-sectarian, and equal opportunity institution.

Legal Framework:

All Email users must operate within the laws of all appropriate jurisdictions that apply, including the Family Educational Rights and Privacy Act of 1974 (FERPA). AUC Email is subject to the full range of laws applying to other communications, including copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification, anti-discrimination legislation, the creation of contractual obligations, and criminal laws.

15. For the purposes of disposal and retention, Email should be treated in the same way as regular mail and paper documents.
16. If required by law, AUC will provide relevant information to law enforcement entities.
17. Abuses of AUC's Email services should be directed to infosec@aucegypt.edu or the Information Security Office.
18. AUC Email users understand and acknowledge that in cases of prosecution or court orders and/or for the purpose of an internal investigation, the University shall have the full right to authorize access to users' email accounts and related data logs.

Guidelines OF USE:

1. Hacking: AUC Email users should be extremely cautious when opening any attachments, clicking on any link, or responding to any Email.
    a. Forms sent via Email from an unknown sender should never be filled out.
    b. Contact IT Help Desk "support@aucegypt.edu" in case of suspecting any received Email
    c. Report suspicious Emails through the "fish" icon on the Email.
2. Password Protection: AUC's policy requires the use of strong passwords for the protection of Emails. Kindly refer to the AUC password policy.
3. Departmental Email Boxes: Departments that provide services via Email should create departmental Email boxes. This departmental Email must have one defined owner, while all targeted recipients in the department can receive Emails through auto-forwarding and send Emails through the "send as" option.

Examples of prohibited uses of Email include but are not limited to:

1. Intentional and unauthorized access to other AUC Email accounts
2. Sending "spam," chain letters, or any other type of widespread unauthorized distribution of unsolicited Emails;
3. Sharing AUC Email addresses lists with anyone who hasn't this right or privilege
4. Use of Email for commercial activities or personal gain, or non-AUC business (except as specifically authorized by University policy and in accord with University procedures)
5. Use of Email for partisan political or lobbying activities.
6. Use of Email for hacking purposes.
7. Creation and use of a false or alias Email address in order to impersonate another or send fraudulent communications.
8. Use of Email to transmit materials in a manner that violates USA & Egyptian Laws and regulations.

9. Use of Email to send inappropriate content
10. Giving the impression you are representing the University unless you are authorized to do so
11. Impersonating someone else.
12. Sharing Email credentials with any party.
13. Forwarding or sharing "this includes associated storage services" any AUC business-related or sensitive information to other non-AUC email or any unauthorized person unless the recipient has to get this information for a valid business need or the recipient entity has signed an official Non-Disclosure Agreement (NDA)

<u>Violation Penalties</u>

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action, up to and including termination of employment or dismissal from the University.

The University has the right to change this policy as necessary without notification.

Forms/Instructions

List applicable forms or other university and external documents that provide helpful, relevant information. Include where these documents can be located.

Related Information

https://www.aucegypt.edu/about/university-policies

History/Revision Dates

Origination Date: May 2014
Last Amended Date: October 2022
Last Review Date: October 2022
Next Review Date: October 2025