جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Electronic Messaging	Last Review date	19/5/2021
	Policy Number	IT-17	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This policy ensures all compliances and protection of official methods of electronic messaging of The University of Sharjah.

Scope

The scope of this policy covers all aspects of electronic messaging at UoS with which users shall abide by while accessing and using the university's information and information system in all locations.

Purpose

The purpose of this policy is to outline expectations for appropriate, safe, and effective electronic messaging use. Application of this policy will reduce and manage the risk of an electronic messaging-related security incident, foster good business communications both internal and external to the University of Sharjah, and to ensure and provide consistent and professional application of University of Sharjah's electronic messaging principles

Policy

Access to University of Sharjah electronic messaging facilities (including employee and student E-mail) is granted to members of the University's community to conduct University business/instruction with the understanding that such access is a privilege and carries with it certain responsibilities. Users of the university-provided electronic messaging capabilities must recognize that these resources are a form of professional communication to which relevant Human Resources policies, and applicable Federal UAE State laws.

As a record, electronic messages require the preservation of their structure, context, and content. Electronic messages must be captured into an identifiable recordkeeping system and where possible directly into an electronic recordkeeping system to ensure effective record management practices. Electronic messages must be readily accessible to meet business and accountability requirements. Electronic messages must be appropriately protected

General:

1. This policy shall regulate the use of the electronic messaging system in The University of Sharjah
2. All use of electronic messages shall be consistent with The University of Sharjah's policies of ethical conduct and safety.

3. The University of Sharjah employees shall only use email and/or other tools that have been approved by The University of Sharjah.
4. The University of Sharjah electronic message account shall be used primarily for The University of Sharjah business-related purposes.

Security Controls:

1. Web access of electronic messaging from untrusted public networks such as public internet café or open wireless networks shall have appropriate security measures.
2. Users are prohibited from triggering automatic or manual forwarding of The University of Sharjah electronic messages to a third-party electronic message system.
3. Any electronic messages found confidential shall have acceptable encryption such as a digital signature.
4. All electronic messages shall be scanned for malicious contents.
5. Electronic messages from unknown links shall not be opened.
6. All electronic message attachments, regardless of the source or content, shall be scanned automatically for viruses and other destructive programs.
7. All malicious electronic messages and attachments shall be quarantined and deleted permanently once the appropriate forensic is accomplished
8. All emails shall have a The University of Sharjah disclaimer appended.
9. If any user leaves The University of Sharjah, access to shall be revoked.
10. An electronic message that is identified as a University of Sharjah business record shall be archived.
11. Anti-malware software shall be installed on email servers including SMTP gateway systems that transact email with the external world. Anti-malware software should be configured to scan attachments in all emails. If malware is found in an incoming SMTP mail, then the following actions should be taken:
    a. Infected attachment should be deleted.
    b. All emails containing attachment with malicious extension shall be automatically blocked and should be replaced with an appropriate warning message:

Reference

Sl NO	Standard Name	Control
1	ISO 27001:2013	A.13.2.3

جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Electronic Messaging	Last Review date	19/5/2021
	Policy Number	IT-17	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs