جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Information Exchange	Last Review date	19/5/2021
	Policy Number	IT-18	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

The objective of the policy is to provide a guideline on the transfer of information and / or internal and external communications to ensure protection of the confidentiality, authenticity and integrity of information.

Scope

This policy applies to all employees, interns, contractors, members, participants, users, and third parties who have access to University of Sharjah information assets regardless of physical location.

Purpose

The purpose of this policy is to protect the exchange of The University of Sharjah enterprise data in transit through various communication applications and media including but not limited to email, texting, messaging, paging, file transfer, virtual private networks (VPNs), application interfaces, and other communication channels.

Policy

All University of Sharjah Employees shall adhere to this policy and ensure that the policy components and requirements set in this document are followed and applied in daily activities for all University of Sharjah data and information system

Information Exchange Policy:

1. The University of Sharjah shall protect the exchange and sharing of University of Sharjah enterprise data.
2. Formal policies, procedures, and controls shall be in place to protect the exchange of The University of Sharjah enterprise data through the use of all forms of communication media.
3. The Management shall define the terms and conditions of electronic communications with other organizations owning, operating, and/or maintaining external information systems.
4. Employees and contractors shall be educated according to the Privacy and Security Awareness, Education processes for safe and approved practices for information exchange.

5. Controls and restrictions shall be implemented to prevent the unauthorized forwarding of electronic communications (e.g., automatic forwarding of email to external email addresses).

Information Exchange Agreements:

1. Information exchange agreements (including the Participation Agreement) shall be established and implemented for the exchange of information and software between The University of Sharjah and third parties.
2. Information exchange agreements should be contractually addressed between the University of Sharjah and third parties or they may be in a separate agreement.
3. Information exchange agreements shall specify the minimum set of controls for responsibilities, procedures, technical standards, technical solutions, incident management, reporting and notification, access controls, auditing, logging and monitoring, and physical safeguards.
4. Information exchange agreements shall specify all applicable The University of Sharjah policies.
5. The University of Sharjah policies, procedures, and standards regarding the protection of the exchange of The University of Sharjah enterprise data shall be referenced in information exchange agreements. Physical Media in Transit:
6. Procedures shall be established and implemented to protect media in its stored physical form (e.g., back-up tapes, USB flash drives, CDs, DVDs, hard drive devices, etc.) while in transit.
7. Physical media containing confidential data shall be protected against unauthorized access, misuse, corruption, or destruction during transportation outside of The University of Sharjah physical boundaries.
8. Controls shall be established to protect confidential data residing on physical media from unauthorized disclosure or modification while in transit.

Electronic Messaging, Texting, and Paging:

1. The information involved in electronic messaging, texting shall be appropriately protected in accordance with The University of Sharjah information security policies.
2. Approval shall be obtained from the IT Director prior to using external public services (e.g., file sharing, etc.) that are not approved by or managed by The University of Sharjah.

3. Electronic messages shall be encrypted throughout the duration of their end-to-end transport path according to the Encryption Policy.
4. Employees, contractors, members, participants, users, and third parties shall never send unencrypted University of Sharjah confidential data via messaging technologies (e.g., email, instant messaging, textual paging, SMS texting, chat, etc.).

Interconnected Information Systems:

1. Policies and procedures shall be developed and implemented to protect confidential data associated with the interconnection of information systems.
2. Security and business implications shall be addressed for interconnecting information assets including:
    a. Policy and appropriate security control to manage information sharing.
    b. Excluding confidential data, if the system does not provide an appropriate level of protection.
    c. Categories of employees, contractors, members, participants, users, and third parties are allowed to use the system and the locations from which it may be accessed.
    d. Restricting selected systems and facilities to specific categories of employees, contractors, members, participants, users, and third parties.
    e. Identifying the status of employees, contractors, members, participants, users, and third parties.