جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Cryptographic Policy	Last Review date	19/5/2021
	Policy Number	IT-16	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

The objective of this policy is to guide understanding encryption and the encryption key management required for maintaining the confidentiality and integrity of the University's confidential.

Scope:

This policy applies to:

1. All individuals, including staff, faculty, students, contractors, and visitors, who have access to the University of Sharjah digital services, information, login credentials, and technologies.
2. All facilities, technologies, and services that are used to process the University of Sharjah information.
3. All information processed, accessed, manipulated, or stored by the University of Sharjah.
4. Internal and external processes that are used to store, transfer or process the University of Sharjah information.
5. External parties and suppliers that provide information storage, hosted systems, transferal, or processing services to the University of Sharjah.

Purpose:

The purpose of this policy is to provide users with information on Cryptographic processes to ensure the protection of the University of Sharjah information and information assets.

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 as relevant.

General:

Information encryption requirement shall be determined and agreed by information owners and custodian (ITC) based on evaluation of information asset criticality in terms of confidentiality, integrity, and authenticity requirements. Refer UoS assets classification and ownership policy.

Cryptographic controls:

1. The information security team shall define the type and the quality of the encryption algorithm required to be used.
2. The information security team in coordination with IT Operational teams shall specify the tools and applications to be used for information encryption.
3. The usage of cryptographic controls shall comply with the latest cryptography standards approved by the Information Security team in coordination with IT Operational teams.

Key Management:

1. Encryption keys shall be generated automatically.
2. Encryption Keys shall be securely stored with authorized personnel. A secure method shall be adopted for key management while using encryption methodologies in the enterprise.
3. Encryption keys are the most sensitive type of information, and access to such keys shall be strictly limited on a need-to-know basis.
4. Cryptographic keys must be generated, stored, and managed in a secure manner that prevents loss, theft, or compromise. Keys need to be communicated by reliable and secure methods and kept confidential. Separate channels should be used for key and data transfer. Under no circumstances should the key and encrypted data be transferred together via the same medium. There must be procedures and controls in place for certificate revocation in the event of compromise or expiry
5. Maintenance of SSL certificates and renewal to be planned -- protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

Usage of Information:

1. Confidential Information stored on removable storage devices shall be encrypted and physically protected.
2. Information classified as confidential being transmitted through email to a different domain email shall be encrypted.
3. All backup information shall be encrypted.
4. For the exchange of confidential information with external entities, digital signatures or similar protection controls shall be used.
5. The key for decrypting information shall be communicated through an alternate method/channel to avoid the compromise of such sensitive information.

Connectivity:

1. All Remote access to information systems shall be provided through secured VPN connections such as IPSEC / SSL-All information is transmitted through wireless networks shall be encrypted using at minimum WPA2 (Wi-Fi Protected Access).
2. Protecting data at rest - encrypting data while it is stored provides effective protection against unauthorized access and theft. Encryption must be used to protect University of Sharjah digital confidential data at rest by default. Any deviation from this policy must be carefully assessed by the Information Security team. Options for encryptions of data at rest include:
    a. Full disk encryption
    b. File encryption
    c. Application encryption
    d. Database encryption
3. University-owned critical devices, or any personal device used for storing University confidential information, must have full-disk encryption enabled by default.
4. Protecting data in transit - encrypting data while in transit provides effective protection against unauthorized interception and access. Encryption must be used to protect University of Sharjah digital data in transit by default. Any deviation from this policy must be carefully assessed by the Information Security team
5. It is important to recognize that even with encryption in place there is a residual risk that sophisticated hacking and decryption methods can still be used to access encrypted files and information. Secure data handling procedures, a as per Information Security Supporting Policies, should always be followed for sensitive and confidential information even whilst that information is encrypted.
6. Encryption must be implemented using approved methods and technologies. Superseded or insecure protocols and cipher suites should not be used unless there is an approved exception in place. Systems, infrastructure, applications, and services must be configured to only accept connections that comply with this requirement.
7. Encryption algorithms and specific implementations of algorithms can contain vulnerabilities. The use of algorithms and encryption software must be monitored and managed through the vulnerability management process by the Information Security team.
8. Certificate Authority must be evaluated carefully. CA is a trusted third party entity that issues digital certificates and manages the public keys and credentials for data encryption for the end user.

9. Key revocation - A revocation key or certificate shall be created in the event the key is compromised. Also, it is required when the access timeframe has expired and sharing of information is no longer required.

Reference

Standard	Control Ref
ISO 27001:2013	**A.10.1.1, A.10.1.2, A.18.1.5**