 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Information Security	Last Review date	3/02/2025
	Policy Number	ITC-19	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

## Overview

UoS is committed to collecting, handling, storing and using Sensitive Information properly and securely. This Policy establishes an Information Security Program to create administrative, technical and physical safeguards for the protection of Information throughout the University.

## Scope

This policy applies to all University of Sharjah faculty, staff, students, and third parties that are directly or indirectly associated by the University of Sharjah or any entity conducting work on behalf of the University of Sharjah that involves the use of information assets owned by the University.

## Purpose

The purpose of this policy is to ensure that the University's information assets are secured to the appropriate degree. These information assets are of significant value to the University. If they are not available when needed or are improperly disclosed, the University could incur serious financial loss or loss of reputation.


## Policy

- All the University of Sharjah faculty, staff, students, and third parties should adhere to this information security policy and the appropriate supporting policies.
- The Information Security and Risk Committee shall oversee an information security program, which shall include information security strategy, principles, policy, objectives, and other relevant components.
- The program shall include means of ensuring that stakeholders within the University are involved in decisions relating to information security.
- The program shall include means for ensuring effective communication in support of information security.
- Management shall allocate sufficient resources and staff attention to adequately address information security.

## Procedures

### 1) Information Asset Classification and Management:

1. All University information assets shall be classified according to the University Information Classification Standard.
2. All University information assets shall have an identified information owner and shall be managed and handled in accordance with the classification standard and related standards, procedures, and guidelines. (refer to UoS Information Classification and Ownership Policy)

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Information Security	Last Review date	3/02/2025
	Policy Number	ITC-19	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

## 2) Roles and Responsibilities

### Users:

1. Information security is every user's responsibility, and the user must understand their specific responsibilities for information security.
2. Users are required to abide by the Acceptable Use Policy. IT service units, Colleges, or research institutes may have additional acceptable use policies for their purposes.

## 3) University Management

1. Managers are responsible for promoting security as a part of standard operating procedures.
2. Managers are responsible for ensuring the prompt adjustment of appropriate system permissions when changes to a user's role or status occur.

## 4) Information Owner

The information owner is responsible for:

1. determining the value of the information;
2. classifying the information according to the classification standard;
3. deciding who can access the information;
4. ensuring that risk assessment for the information assets are performed;
5. These responsibilities shall not be delegated by the information owner.

## 5) Information Security Section Head


1. The Information Security Officer is responsible for establishing and maintaining University-wide information security standards, procedures, and guidelines that support the Information Security Program.
2. The Information Security Officer is authorized to review any aspect of any University information system to ensure the security of University information assets.
3. The Information Security Officer is responsible for providing advice and guidance to inform owners when exercising their responsibilities.

## 6) Access to Information Assets

1. Physical and electronic access to University information assets shall be consistently controlled in a manner appropriate with the assets' classification, and access privileges of all users shall be defined based on their assigned roles and demonstrated need for access.
2. Access privileges shall be granted only with appropriate authorization by the information owner along with the review and approval of the security section head.

## 7) Information Security Awareness and Training

Information security awareness and training relevant to each person's role shall be provided to all faculty, students, or other users. Periodically updated training shall also be provided.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Information Security	Last Review date	3/02/2025
	Policy Number	ITC-19	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

## 8) Operation of Information Systems

1. New information systems shall conform to information security standards before being installed into any production environment.
2. Information security standards and requirements shall be included in product specifications during the procurement process.
3. Information systems infrastructure and operating procedures shall be documented, managed, and maintained to ensure conformance with information security standards.
4. All third-party service providers and agents with access to any University information asset shall comply with all regulatory, legal, and contractual requirements, including University statutes and policy documents.
5. When changes are made to systems that may affect the security of information assets, risks shall be assessed, and the system must subsequently conform to information security standards. (ref. Change Management policy)

## 9) Incident Management and Response

1. An information systems disaster recovery plan shall be developed, maintained, and tested in a manner that ensures the ability of the University to continue operations as required by the University's business continuity plan.
2. Security incident reporting and response procedures shall be developed and maintained by the Information Security head, and published and accessible as appropriate. Users shall be informed of procedures relevant to them.

## 10) Physical Security

The Information Security Policy applies to information assets regardless of their media (for example, printed records and paper forms as well as electronically saved documents).

## 11) Privacy Expectations

At any time and without prior notice, University management reserves the right to monitor, access, inspect or disclose any information stored on or transmitted through University information systems. The users' rights to privacy will be respected and disruption to the users' legitimate activities avoided where possible.

## References

Standard	Control Ref
ISO 27001:2013	Clause 5.2