 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Assets Management	Last Review date	10/05/2024
	Policy Number	ITC-05	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

This policy puts the outline for acceptable approach to classify university information assets into risk levels to facilitate the determination of access authorization and appropriate security control. The value of data as an institutional resource increase through its widespread and appropriate use; its value diminishes through misuse, misinterpretation, or unnecessary restrictions to its access.

Scope

This policy applies to all University activity and all University-owned or operated assets including IT systems and software as well as all items of a physical or tangible nature including attractive and portable items; inventory; cultural and/or scientific collections; and Library collections.

Purpose

The purpose of this policy is to:

- Provide a long-term vision for the University's practice of asset management.
- Ensure that asset management aligns with the wider vision and strategic goals of the University.
- Mandate the responsibilities of, and generate useful dialogue between, asset users and ITC.
- Allow for "ease of maintenance" factors to be considered in the design stage.
- Align, support and inform the rebuild programs


Policy

- The University recognizes the importance of protecting and managing Information Assets.
- UoS assets managements and system should support University operations and teaching, scholarly, research, and clinical activities.
- The UoS Assets management system comply with applicable standards, legal, contractual, policy, and other requirements.
- UoS owned the assets system to enable informed decision making, preserve Information Assets for archival purposes and facilitate collaboration and accountability.

Procedures

Information Asset Labelling and Handling

1. All information shall be labeled and handled as per The University of Sharjah Information Classification and Ownership Policy categories to protect it from unauthorized disclosure or misuse.
2. Physical labeling of documents and removable media shall include appropriate security classifications.
3. All information assets including data and documents shall be processed and stored strictly following the classification levels assigned to them.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Assets Management	Last Review date	10/05/2024
	Policy Number	ITC-05	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs


4. Any non-public /open information asset on media or documents shall be stored in fireproof and locked cabinets.
5. All media devices being transported shall be protected from unauthorized access, misuse, or corruption.
6. Non-public /open information asset documents stored in soft copy format shall be adequately safeguarded by the information owner through methods like password protection or encryption as deemed appropriate.
7. Non-public /open information asset must be delivered in a sealed envelope, clearly classified, and only handed over to the staff, it is intended
8. information should be treated with the highest degree of sensitivity at all times.
9. No information regarding any account should be revealed to an unauthorized person.

Removable Media Management

1. Removable computer media shall be controlled and physically protected to prevent interruptions to business operations.
2. Removable computer media shall be stored in a secure environment and accordance with the manufacturer's specifications.
3. Previous contents of any re-usable media shall be completely erased before handing it to the next custodian.
4. Wherever mandated, cryptographic techniques shall be applied to protect data on removable media.

Secure Information Asset Disposal

1. Asset disposal shall be applicable for:
 - a. Physical copy documents.
 - b. Hardware (Media, Hard Disks, laptops, and desktops.)
2. Physical Copy documents:
 - a. A physical copy of obsolete the University's information shall be shredded based on the classification of information and the retention period defined.
 - b. Any Non-public /open information asset that needs to be discarded shall have the authorization of the information owner for discarding.
3. Hardware Assets:
 - a. All equipment containing storage media (e.g. hard drives) shall be checked to ensure that any critical business information assets and licensed software are removed, securely overwritten, or destroyed before disposal.
 - b. Hard Disks shall be degaussed or physically destroyed.
4. Before disposing of asset media, it shall be sanitized by reformatting the hard drive in a secure manner or by using a wipeout utility.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Assets Management	Last Review date	10/05/2024
	Policy Number	ITC-05	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs


5. Tapes and other magnetic storage media that contain University data or software shall be sanitized when they are no longer needed.
6. Inoperable magnetic media & optical media shall be physically destroyed.
7. Media destruction techniques below can be considered:
 - a. Pulverizing: Media is shattered or ground into small non-constructible pieces.
 - b. Degaussing: Erase Magnetic tapes through an electromagnetic field.
 - c. Abrasion: Media is destroyed using an abrasive device to rub away the recording surface.
8. Hardware assets sent outside The university for repair or data recovery shall be protected from disclosure of information by a mutually agreed contract.
9. It is the responsibility of each department to ensure that the all University of Sharjah and personal information are deleted before disposal of the media.

Information Asset Management Committee

1. The Information Asset Management Committee is comprised of one representative from each of the following:
2. legal services
3. ITC
4. archives
5. records management
6. the Research and Scholarship Committee of the General Faculties, as determined by that committee
7. Academic committee

The Information Asset Management Committee will oversee the management and protection of Information Assets including:

1. Establishing and review operating standards and practices relating to the receipt, creation, storage, handling, protection, and disposition of Information Assets.
2. Identifying legal, policy, and other requirements relating to the management and protection of Information Assets.
3. Risk assessment and compliance activities relating to the management and protection of Information Assets.
4. Information Custodians will manage physical or electronic systems that receive, create, store, handle or dispose of Information Assets following University policies, operating standards and practices, and legal and other requirements. Identification and Classification of Information Assets
5. Assets custodians will identify and classify Business Information Assets and Health Information Assets following The University of Sharjah and the Information Security Classification Standard.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Assets Management	Last Review date	10/05/2024
	Policy Number	ITC-05	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Retention and Disposition of Information Assets

Information Assets are retained and disposed of following the rules published by the concerned department. The following factors are considered when determining retention and disposition rules for Business Information Assets:

1. statutory and other legal requirements
2. administrative requirements and archival value.
3. The following factors are considered when determining retention and disposition rules for Scholarly Information Assets and Health Information Assets:
 4. statutory and other legal requirements;
 5. research value and archival value.
 6. Retention and disposition rules for Information Assets will be approved by ITC.
 7. Retention periods will be extended by the University's General Counsel for Business Information Assets that are required for:
 8. an ongoing or pending dispute, grievance, claim, or litigation on behalf of or against the University
 9. a criminal investigation
 10. an ongoing or pending protected disclosure investigation
 11. an ongoing or pending audit
 12. ongoing or pending access to information request filed under FOIP or other applicable legislation.
 13. Information Assets that must be retained for a purpose will be retained for the period determined by the University's Management.

Protection

Information Assets stored in electronic form on University-managed systems will be protected, to the extent reasonably possible, against storage media deterioration and software and hardware obsolescence.

Reference

SI NO	Standard Name	Control Reference
1	ISO 27001:2013	A.8.1.1,A.8.1.2,A.8.1.3,A.8.1.4