 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Physical Security	Last Review date	10/05/2024
	Policy Number	ITC-25	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and administrative Affairs

Overview

This document establishes a standard set of rules and requirements that help manage and control the physical security of the University of Sharjah information and information processing facilities. It is intended to protect the security of UOS data and technology infrastructure.

Scope


This policy is applicable to UOS Faculty, employees and students including but not limited to, contractors, third party users, consultants, and temporary users at UOS who wish to access the university's information assets.

Purpose

This Physical Security Policy shall ensure that access to information, information processing facilities, and business processes are controlled on the basis of business / academic IT requirements in UOS.

Policy

- Physical access to UOS premises containing critical network infrastructure and information resources shall be protected by appropriate electronic access, such as Biometric Controls.
- Access to UOS premises shall be given in accordance with "Access Control Policy".
- All UOS employees shall wear their ID card while in university premises
- All sites where computers and servers are located shall be appropriately protected from environmental hazards and manual threats.
- UOS shall maintain visitor's log book for all visitors that shall include following information:
 - a. Visitor's name and organization
 - b. Date of access
 - c. Time of arrival and departure
 - d. Form of identification presented and verified
 - e. Name and organization of person being visited
- All secure areas in UOS premises shall have emergency evacuation plan along with clearly marked secure emergency exit doors.
- Centralized air conditioning units will be used to monitor the temperature of the computer room.
- Adequate safety devices e.g. fire alarm, smoke detector, etc. shall be placed in all UOS areas.
- Regular fire drills shall take place to measure the effectiveness of the evacuation plans.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Physical Security	Last Review date	10/05/2024
	Policy Number	ITC-25	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and administrative Affairs

Procedures

Securing Offices, Data Center and Facilities


1. Computer (Data) Centers shall be located within the UOS.
2. Access to all secure areas shall be logged. These logs should be protected, monitored and reviewed periodically.
3. Anyone escorting a visitor to a Data Centre shall be held accountable for their role as a security escort.
4. All data centers, equipment rooms, and telecommunications closets shall be locked when unattended. The key will be kept with the accountable personnel.
5. Network devices such as routers, switches, and hubs shall be placed in restricted access zones that provide protection from unauthorized or unnecessary access and from any environmental hazards.
6. All application and/or database servers shall reside in a Computer (data) Center.
7. All source media for operating system software, applications, backup tapes/devices and license keys shall be kept in fireproof locked area.
8. Support functions and equipment such as photocopiers and fax machines should be protected from unauthorized access.
9. No combustible or hazardous materials should be allowed in restricted zones.
10. Temperature and humidity in the data center and other information processing areas shall be controlled, monitored and maintained using adequate air and humidity controlling equipment.
11. The environmental security equipment shall undergo regular maintenance as per the manufacturer's recommendations and records shall be maintained.
12. Supplies such as stationery shall not be stored in the data center and equipment rooms.

Delivery and Loading Areas

1. Wherever possible, delivery and loading areas shall be isolated from the information resources.
2. Materials, supplies and equipment entering and leaving UOS premises shall be inspected and where necessary registered.
3. All the equipment and information assets shall be brought inside the premises as per authorization from the respective asset owner.
4. Measures shall be taken to inspect and examine all incoming materials for explosives, chemicals or other hazardous materials.

Equipment Security

1. Equipment shall be placed in a location adequate to its criticality and its classification.
2. Equipment shall be protected from environmental threats and hazards and opportunities for unauthorized access.
3. Equipment shall not be moved from its location unless authorized.
4. Equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.
5. All newly acquired equipment shall be classified as per the Asset Classification Policy

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Physical Security	Last Review date	10/05/2024
	Policy Number	ITC-25	Next Review date	10/03/2028
	Responsible Entity	Director of ITC	Approved By	Vice Chancellor for Financial and administrative Affairs

Supporting Utilities

1. Equipment shall be protected from power failures and electrical anomalies.
2. Electrical supply shall conform to the manufacturer's specifications for each piece of equipment.
3. Critical equipment shall be supported by uninterruptible power supply (UPS).
4. UPS, batteries and power supply equipment shall be placed in an isolated place secured from unauthorized access.

Cabling Security

1. Power and telecommunications cables carrying data or supporting information services shall be protected from interception or damage.
2. Power and telecommunications lines into the premises and server room shall be adequately protected.
3. Network cabling shall be protected from unauthorized interception or damage.
4. Power cables shall be segregated from communications cables to prevent interference.

Secure Disposal or Re-Use of Equipment

1. No equipment shall be disposed without authorization from the management.
2. Proper disposal procedure shall be followed in case of information assets and systems being removed from UOS facility

Reference

SI No	Standard Name	Control Reference
1	ISO 27001:2013	A.6.2.1, A.13.1.1, A.13.2.1