جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Access Management	Last Review date	19/5/2021
	Policy Number	IT-02	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

The users' access control policy applies to all staffs, faculty members, students, contractors, consultants, suppliers, vendors, partners, and customers of the University of Sharjah who are using and accessing data and information system in all locations.

Scope

The scope of this policy covers all users accessing and using University of Sharjah's data and information systems, processing facilities, networks and equipment.

Purpose

The purpose of this policy is to ensure that both logical and physical access to UoS information assets are granted to users on asset classification and 'need-to-know' basis. The policy also establishes control statements and processes that addresses authorization, modification, revoking access and periodic reviews of access granted to users.

Policy

General

1. No access shall be granted to information technology resources unless authorized by relevant system owner.
2. Any addition/ modification of access shall be approved by the system owner.
3. Unique User ID shall be created for each user.
4. All access privileges shall be reviewed periodically.

User Access Provisioning

1. All user access shall be role based and granted only on need to know basis.
2. Access to the University of Sharjah's information services shall be controlled through a formal user registration process.
3. Every access shall have a formal request raised and shall be approved by the respective manager. This shall be applicable to:
    a. New Hire
    b. Change of employment
    c. Temporary Access
    d. External User Access

The request shall be actioned by the IT center based on the nature of the request and as per Identity access management agreed workflow.

Based on the criticality of the information and the confidentiality involved, the access shall be approved by the Department head/ Information Owner and endorsed by ITC director

a. Each user shall have a unique user ID created and assigned. Generic IDs shall be documented and ownership assigned to track accountability.
b. All Email Ids shall be created in a unique predefined format.
c. Once the IDs are created, the password to the users shall be shared in a secure manner.
d. All passwords shall be configured to change on the first logon.

Privilege Access Management

1. Privileged access shall only be provided to users who are assigned by the department to modify configurations and manage infrastructure.
2. All privilege access requests shall be approved by the section head and verified by ITC director.
3. A list of privileged access users shall be available with ITC and the department requesting access. Privileged accounts must have multi factor authentication.

Access Reviews

1. All users' access shall be reviewed by the respective department at least once in 6 months.
2. Privilege Access reviews shall be done at least once in 3 months.

Alumni

Accounts of all former students will remain on the user registration system only for an approved time period for limited services.

Local Admin Accounts

UoS PC/Laptop users shall not have Local admin access. Only relevant IT team members can have local admin access. Any exception need to be prior to approval and audit tracked with automated solutions.

Change of Role

1. Department Line Managers/ HR shall initiate the request to the ITC to update the change of role of the user.
2. Access to information shall be revoked/ modified if the role of the user is changed.

3. For users changing departments / units, the access to previous information shall be revoked.
4. Any access required for operations in the new department/ unit shall be granted only after respective approvals from the manager and Unit Head.

Termination and User De-Provisioning

1. Any individual leaving the University of Sharjah's employment shall have system credentials revoked.
2. Once the user resigns, HR shall initiate the request to ITC to revoke logical access and the Physical Security Team to revoke physical access of the user. (Ref. UoS Wireless Policy, UoS Network policy).
3. Access to critical information shall be disabled during the employee notice period.
4. IT operations shall delete network access and services on the last day of the employee.
5. The login ID and email Address shall be deleted on the last day of the employee.
6. If the email address/ Login ID needs to be retained for business purpose, then an approval from the Chancellor shall be taken.
7. Any temporary access shall be revoked after completion of the activities.

Network Access

1. No devices shall be allowed to connect to University of Sharjah's network unless approved.
2. For external Connections, authentication shall be mandated before connecting to university's network.
3. Access to network configuration ports shall be controlled.
4. Segregation of network shall be done to separate processing facilities containing critical information.

Operating Systems Access Control

1. Secure Log-on controls shall be implemented to ensure secure connectivity to operating systems.
2. Session time-out shall be implemented wherever applicable.
3. Account lockout policy shall be implemented on all systems.
4. Connection lockout time to application / systems shall be implemented wherever applicable.

5. Logs will be enabled and archived for all critical systems. Local users shall not be created without ITC consent.

Application Access

1. Role-based access shall be applied to all applications. This shall be based on the business / academic requirement.
2. Critical systems shall be segregated logically and physically.

Reference

Standard	Control
ISO 27001:2013	A.9.2.1; A.9.2.2; A.9.2.3; A.9.2.5; A.9.2.6