جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Authentication	Last Review date	19/5/2021
	Policy Number	IT-07	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

This policy is for the University of Sharjah access accounts administered by the Information Services. These access accounts are the user ID and password used for all systems maintained by The University of Sharjah that utilize these credentials for authentication and authorization.

Scope

The scope of this policy includes all Faculty, employees, students and third party users of UoS information assets and processing facilities who have accounts (or any form of access that supports or requires a password) on any UoS system.

Purpose

Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents their compromise.

Policy

The policy is developed and maintained to provide governing statements regarding any information security key process, through setting the rules for expected behavior by users, systems administrators, management, and end-users; authorize security personnel to monitor, probe, and investigate; define and authorize the consequences of the violation; define the entity consensus baseline stance on security; help minimize risk; and help track compliance with regulations and legislation.

Password Usage Responsibilities:

1. Passwords shall be kept confidential and shall be owned by respective Individuals of the system. Password security is an individual responsibility and failure to abide by this policy shall result in disciplinary action.
2. All The University of Sharjah information systems shall require identification and authentication through passwords, pass-phrases, PINs, one-time passwords, and similar password mechanisms as a minimum (A more restrictive /secure authentication mechanism is acceptable) before allowing user access.
3. Users are responsible and liable for all actions including transactions, information retrieval, or communication performed on The University of Sharjah information systems by using their user-id(s) and password(s).

4. If a user forgets his / her password, then he/she shall contact "ITC service desk", who shall provide a password reset after evaluating the user's credentials and employee records.
5. Users shall not enable the "Remember Password" feature on applications, websites, or web browsers.
6. Users shall restrict from using easily guessable passwords such as family members' names, pets, or popular places.
7. The use of generic IDs or group accounts is prohibited to ensure accountability. In case of a business, need arises for such usage, one user from the group shall be identified as responsible for all activities carried out using these accounts.

Password Management:

All user-level and system-level passwords shall conform to the guidelines described below:

1. The password minimum length should be 8 characters (no maximum limitation).
2. Complex password must contain characters from three of the following categories:
    a. Uppercase letters (A-Z).
    b. Lowercase letters (a-z).
    c. Numbers (0 - 9).
3. Non-alphanumeric characters: ~!,@#$%^&*_-+=`|(){}[]:;"'<>,.?/.
4. The Password shall be Case Sensitive.
5. The password must not contain the user's user name.
6. The user shall be forced to change his/her password every 3 months.
7. Password History – 5 (. i.e. the user cannot repeat the last 5 passwords).
8. For administrator and privileged users, the password shall be at least 14 characters with complex requirements enabled. Must contain at least 4 characters from the following:
    a. Uppercase and Lower case.
    b. Numeric (0-9).
    c. Non Alpha Numeric (e.g. @#$%^&*() _+|~-=\` {}[]:";'<>/).
    d. Must not contain 3 or more characters from the username.
    e. Must not contain 4 or more repeating characters.
9. For administrator and privileged users, the password shall be changed after 45 days or whenever an employee of the team leaves the department.
10. Systems shall be configured to ensure that the initial, temporary passwords for newly allocated accounts are changed at the first login.
11. Default vendor passwords shall be changed after the installation of any third-party device.

12. Temporary passwords shall be given to users securely. Temporary passwords shall also be unique to individuals and not easily guessable.

Account lockout:

1. On inactive sessions, the system shall be locked within 15 minutes.
2. Accounts shall be locked after five unsuccessful tries. The account shall be unlocked after 5 minutes and locking and unlocking shall be logged.

External Users Authentication:

1. All external access to The University of Sharjah network shall have an authentication mechanism.
2. All External users accessing The University's Information Processing environment, from within The University of Sharjah or from some other external location, must be provided with a unique user-id and password to maintain accountability.
3. External users shall follow The University of Sharjah authentication policy for IDs created for them on Active Directory.
4. For external users who access through web applications for supporting users and accessing through a mirroring function, monitoring and logging of activities should be enabled at all times.
5. External vendors shall have an agreement inclusive of a Non-Disclosure Agreement mutually agreed and signed before granted authentication access to use any University's network.

Authentication policy Implementation:

1. All default passwords on systems, applications, databases, and devices shall be changed immediately after the first login.
2. All applications procured or developed for The University of Sharjah shall have the capability to enforce The University of Sharjah's Authentication policy and this shall be taken care of during the development stage/procurement stage itself.
3. Administrator/root password shall not be used for day-to-day activities.
4. Root and admin password shall be changed as per the policy and kept in a sealed envelope in a fireproof safe under the custody of Head of Units / Sections. Emergency usage of such passwords shall be recorded and changed after the usage wherever possible.
5. Tiered administrative levels must be followed for core IAM service such as AD and ERP.

6. Whenever possible, applications must use UOS's centralized authentication and authorization infrastructure.
7. Applications must avoid implementation of 'ad hoc' authentication and authorization processes. Where this cannot be avoided, the Director of Information Technology must approve the processes adopted

Reference

Standard	Control
ISO 27001:2013	A.9.3.1, A.9.4.3