The Knowledge Hub
Universities

Document title: [Password Security Policy – September 2019]
Document version number: V.1
Office/department responsible: IT Department
Approved by: Dr. Mahmoud Allam – President of The Knowledge Hub Universities

---

Who Needs to Know This Policy

Entire TKH Community

The scope of this policy includes all Operating systems, Applications, Databases and Network devices of TKH. It also includes personnel who have an account (or any form of access that supports or requires a password) on any system that related to TKH systems.

Supporting Department

Responsible University Official: Khaled Mubarek – IT Manager
If you have any question about this policy, please send an email to:
khaled.mubarek@elsewedyedu.com

Policy Statement/Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, protection of the passwords and to define the frequency of change.

Policy/Procedures

1.1 Password Policy Statements

1.1.1 Password Usage Responsibilities

1. All users of TKH information systems shall abide by the Password Policy. Password security is an individual responsibility and failure to abide by this policy shall result in disciplinary action.
2. All TKH information systems shall require identification and authentication through passwords, pass-phrases, one-time passwords and similar password mechanisms as a minimum (A more restrictive /secure authentication mechanism is acceptable) prior to allowing user access.
3. TKH information systems (access control programs) shall be configured (where such configuration is possible) to fulfil the requirements of this policy and TKH password rules, guidelines and procedures.
4. Passwords shall be regarded as confidential information and shall not be disclosed to any other person except in accordance with TKH password management procedures for safekeeping of passwords.

5. Users are responsible and liable for all actions including transactions, information retrieval or communication on TKH information systems performed by using their user-id(s) and password(s).

1.1.2 Password Validity Policy

1. All system-level and production environment passwords (e.g., root, admin, application administration accounts, Network and security devices, appliances etc.) shall be changed at regular intervals as recommended by Systems Admins.
2. All user-level passwords (e.g., application user, email, web, domain and individual desktops and laptops etc.) shall be changed at least once every 60 days.

1.1.3 Password Uniqueness Policy

1. User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from all other accounts held by that user.
2. Passwords shall be checked to ensure that they are not identical to any of the previous 3 passwords for the same account.

1.1.4 Password Composition and Strength

1. All user-level and system-level passwords shall conform to the guidelines described below: -
    - User-level passwords and Administrator / privilege level passwords shall be at least 8 characters long with alpha-numeric and special characters.
2. Passwords shall never be written down or stored on-line.

1.1.5 Password Management

1. Initial passwords shall only be valid for the first log-on.
2. All users shall change their temporary password at first login.
3. In case of forgotten passwords, temporary passwords shall be issued only after positive identification of the user.
4. All passwords relevant to the administrators, backup administrators, supervisors, super users, root etc., who has resigned or has been terminated or transferred, shall be changed immediately.

1.1.6 Passwords Policy Implementation

1. All systems that are not part of the central domain of TKH shall have password policy implemented at the local level.
2. Passwords shall be checked automatically by the system itself to ensure they are sufficiently complex. Routine password auditing shall be performed by the IT department to ensure compliance with these standards.

3. The administrator / root password shall not be used for day to day activities. The root and admin password shall be changed as per the policy
4. The following password syntax rules shall be followed and apply to all administrative Logon passwords and of all devices in TKH facilities. The relevant operating systems, applications, database and all devices shall be set to enforce these rules to the extent that they are capable:
    a. Be at least 8 characters in length.
    b. Contain alpha-numeric and one special character.
    c. Not contain the user ID as part of the password.
    d. Be changed at least once every 60 days.
    e. Not be reused until after at least three iterations.
    f. Have a minimum password age of 1 day.

History/Revision Dates
Origination Date: September, 2019
Next Review Date: December, 2019

*****Disclaimer:** The Knowledge Hub Universities reviews the policies on regular basis if needed for work flow and business purposes.

Version Log	Date	Signature of the President of TKH
Version 1 (V.1)		