The Knowledge Hub
Universities

Document title: [TKH IT Security access control 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

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

This policy is applicable to all systems, and information processing facilities, personnel as well as all third-party personnel who are using TKH systems.

The purpose of access control policy is

1. To establish security requirements to have controlled access to the information assets of TKH, to ensure that information remains accurate, confidential and available when required.
2. To ensure that user registration and de-registration is controlled, authorized, and a record is maintained.
3. To ensure that the access is role based for common categories of jobs.
4. To ensure that privileges granted is restricted and controlled.
5. To ensure that the allocation of passwords is controlled, and user access rights are reviewed regularly.

1.1 Access Control Policy

1.1.1 Access Control Requirements

1. Access to TKH information and information systems shall be granted based on an identified business requirement for the user to have access to the information or business process and shall be granted on a ‘need to know’ basis only.

2. All information and system access requests shall be authorized by the respective business unit head and HR.

3. All assets containing TKH information shall have capability to enforce access control rules based on the TKH IT security requirement and all assets shall be configured with specific access control rules as per the business requirements only.

1.1.2 User Creation

1. All TKH information users shall have unique user IDs for accessing any system / application belonging to TKH.
2. Each user ID shall be identifiable to an individual except when the technical limitations of the operating system require the sharing of an administrative ID, redundant User-ID's shall not be issued to any user.
3. A standard naming convention for User ID creation shall be followed which is First Name - Last Name unless stated differently for business requirement or common names.

1.1.3 User Deregistration

Information Owners and Custodians must formally assign responsibilities and implement a process to:

1. Review Access Rights whenever a TKH Employee's duties and Responsibilities change.
2. Remove Access privileges for employees terminated for a cause concurrent with the notification to the individual.
3. Review User account privileges of personnel transferred to a different TKH Department by HR and to be sent to IT department to take necessary actions.
4. User accounts of personnel leaving TKH shall be disabled immediately or removed.

1.1.4 Third Party Access

1. All Third-party personnel (contractors, vendors, consultants, etc.,) requiring access to TKH's information systems shall follow TKH access Control Procedure for registration to access TKH's Information Assets.
2. Access for contractors, consultants, or vendor personnel to TKH Information assets shall be provided only on the basis of a contractual agreement. This agreement shall provide:
    - The terms and conditions under which access is provided.
    - The responsibilities of the contractors, consultants or vendor personnel.
    - Agreement by the contractors, consultants or vendor personnel to abide by TKH Information Security Policies. These instructions shall include security requirements, such as the need to maintain the confidentiality of the information, requirements for distribution of the information, and procedures for destruction or return of the information following the period of access.

1.1.5 Privileged Accounts

1. Privileged accounts provide higher levels of access for individuals who perform system administration and User Account Maintenance functions or personnel who administer restricted information resources.
2. Privileged accounts shall be used in accordance with the following guidelines:
    - Assignment must be restricted to personnel whose duties require additional privileges.
    - Privileged accounts must be assigned to a unique individual.

  - A user with a privileged account is restricted to perform only those job functions required by the privileged account, individuals must use their regular user accounts to perform non privileged functions.
  - The number of privileged accounts to any information system must be kept to a minimum.
  - An Audit trail must be maintained on all privileged account usage.

3. Administrator Account shall not be used for Emails, Internet browsing etc.

1.1.6 Shared Accounts

Shared accounts have a single logon ID and are used by more than one person. Establishment of shared accounts if necessary / is a business requirement shall meet the following criteria:

- Shared accounts must be placed under strict Management control.
- Requesting Manager is responsible for use of the Shared Accounts.
- The Requesting Manager must control access to the password.

1.1.7 User Rights Management

1. All rights to the users shall be assigned through a formal authorization procedure.
2. All user rights shall be allocated as and when required on a need to know basis and detailed records shall be maintained for all the privileges / rights allocated.
3. On creation of user accounts or resources, the default access shall be limited to the owner only.
4. Third party personnel and customers accessing TKH Systems and IT resources shall be provided access only to the information and services they are authorized to access.

1.1.8 Unattended User Equipment

1. All users and relevant administrators shall enable password-protected screen savers on user desktops, portable computers/laptops, and servers. The user should set the timer to enable the screen saver after not more than 10 minutes of inactivity. Wherever possible this shall be enforced from the central server such as domain controller.
2. Each user shall terminate active sessions when activities are finished and for production systems and equipment, users shall log off after completion of their tasks.

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

*****<u>Disclaimer:</u>** 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)		