Dundalk Institute of Technology

Logical Access Policy

Version 1.0.3

Document Location

..\DkIT_Policy_Documents\Procedures

Revision History

Date of this revision: 01/11/18	Date of next revision:

Revision Number	Revision Date	Summary of Changes	Changes marked
V1.0	23/07/15	New policy document	
V1.0.1	18/11/15	Review Document	
V1.0.2	07/09/18	Review document for GDPR	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
V1.0.2	07/09/18	James McCahill Loretto Gaughran	Review document for General Data Protection Regulation - GDPR go-live
V1.0.3	01/11/18	James McCahill Michael Denihan	Review document for General Data Protection Regulation compliance

Approval

This document requires the following approvals:

Name	Title	Date
James McCahill	IT Strategy Manager	01/11/18
Michael Denihan	Computer Services Manager	01/11/18

This Logical Access Policy will be reviewed on a periodic basis.

Table of Contents

1 Overview

The Institute is responsible for the provision of IT services to its staff and students.

To make this possible it must manage user access to its systems applications and web services with security and data protection in mind.

2 Purpose

The purpose of this policy is to establish an Information Technology (IT) Logical Access Policy suitable for supporting the security requirements of Dundalk Institute of Technology.

This guideline describes methodologies to use when implementing the logical access control requirements for Dundalk IT resources

Effective implementation of this policy will minimise unauthorised access to these IT systems and services and provide more effective auditing of access controls by:

- Identifying policies and procedures used for logical access to system for granting user access, control, monitoring, and removal of access to ICT facilities
- The procedures for periodic review of Dundalk Institute of Technology users i.e. staff, students, contractors and guests and their access rights.

3 Definitions

User – A user is an individual or group that require access to the Dundalk Institute of Technology network, systems and/or applications to allow them to fulfil their job functions.

Access- Access may be the means / method off access to Dundalk Institute of Technology ICT facilities either by using authorised access control channels (Local PC access, Web access etc.).

4 Roles and responsibilities

IT Manager	• To monitor compliance with the logical access procedure. • To inform the Vice President for Financial and Corporate Affairs of suspected non-compliance and/or suspected breaches of the physical access procedure.
IT Department	• Is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

5 Scope

Logical access controls are a technical means of implementing access policies i.e. interactions with computer systems & data through access control systems which usually feature identification, authentication and authorisation protocols.

Development of the access policies should be directed by the IT Manager with the assistance of the system owners, and data owners.

Development of such policies requires balancing the interests of security (sensitivity and risk) against what is needed to accomplish the day-to-day activities in respect of operational requirements, user-friendliness, and cost.

6 Logical Access Policy

Physical access control protects IT systems through physical barriers. Logical access control protects IT systems and data by verifying and validating authorised users and allowing authorised user access to IT systems and data, and restricting transactions (read, write, execute, delete) according to the user's role and authorisation level.

6.1 Logical Access Authorisation

Logical Access controls encompass the following disciplines

1. Account management
2. Password management
3. Remote Access management

6.1.1 Account Management

Effective account management is central to providing Logical Access control appropriate to the level of sensitivity and risk involved.

It consists of the processes of requesting, authorising, administering, and terminating accounts which access IT systems and data in compliance with GDPR requirements.

This aspect is covered in the user administration setup document "User Administration Procedure.docx".

6.1.2 Password Management

Passwords are required for accounts on all IT systems and are mandatory for accessing all IT systems.

DkIT has documented its own password standard “Password Standard.docx” This document includes requirements for IT Logical Access Control Guideline password policy for access to the DkIT Network and outlines a password standard for the main application systems used in DkIT.

6.1.3 Remote Access

Remote access to sensitive IT systems and data may present serious risks to DkIT.

All remote access to sensitive IT systems and data must be via the encrypted Citrix VPN connection. The encryption must begin with the initiation of the session, include all user identification and authentication, and not end until the session is terminated.

A remote access policy document “Remote Access Policy.Docx” outlines user access and management activities that are identified for different types of users that need to access IT systems outlined in that document

6.2 Logical Access Reviews

Logical access reviews which encompasses managing user authorisation access and remote access reviews) are scheduled twice a year by the IT department. These processes are outlined in their respective documentation.

6.3 Review Responsibilities:

The IT department

The IT Manager will be responsible for ensuring that the logical access review is carried out in conjunction with the Senior Technical officers.