Logical Access Policy

Dundalk Institute of Technology

Logical Access Policy

Version 1.0
Document Location

..\DkIT_Policy_Documents\Procedures

Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Revision Date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>23/7/2015</td>
<td>New policy document</td>
<td></td>
</tr>
<tr>
<td>V1.0.1</td>
<td>18/11/15</td>
<td>Review Document</td>
<td></td>
</tr>
</tbody>
</table>

Approval

This document requires the following approvals:

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>James McCahill</td>
<td>IT Strategy Manager</td>
<td>18/11/15</td>
</tr>
<tr>
<td>Michael Denihan</td>
<td>Computer Services Manager</td>
<td>18/11/15</td>
</tr>
<tr>
<td>Peter McGrath</td>
<td>Vice President for Finance &amp; Corporate Affairs</td>
<td>19/01/16</td>
</tr>
</tbody>
</table>

This Logical Access Policy will be reviewed on a periodic basis.
Table of Contents
1 PURPOSE ........................................................................................................................................... 4
2 ROLES AND RESPONSIBILITIES .................................................................................................... 4
3 DEFINITIONS...................................................................................................................................... 4
4 SCOPE............................................................................................................................................... 4
5 Logical Access Procedure ................................................................................................................. 5
  5.1 Logical Access Authorisation........................................................................................................ 5
  5.1.1 Account Management............................................................................................................... 5
  5.1.2 Password Management............................................................................................................ 5
  5.1.3 Remote Access....................................................................................................................... 6
  5.2 Logical Access Reviews................................................................................................................ 6
  5.3 Review Responsibilities................................................................................................................ 6
1 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.

2 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.

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 of access to Dundalk Institute of Technology ICT facilities either by using authorised access control channels (Local PC access, Web access etc.).

4 SCOPE

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.

5 Logical Access Procedure

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

5.1 Logical Access Authorisation

Logical Access controls encompass the following disciplines:

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

5.1.1 Account Management
Effective account management is central to providing Logical Access control commensurate with sensitivity and risk.

It consists of the processes of requesting, authorising, administering, and terminating accounts which access IT systems and data,

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

5.1.2 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 also outlines password standard for the main Application systems used in DkIT.
5.1.3 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 encrypted. 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 in that document.

5.2 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.

5.3 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.