Dundalk Institute of Technology

Password Standard

Version 1.0.3

Document Location

..\DkIT_Policy_Documents\Standards and Guidelines

Revision History

Date of this revision: 06/11/2019	Date of next revision:

Revision Number	Revision Date	Summary of Changes	Changes marked
V1.0	31/08/2015	Finalising document	
V1.0.1	18/11/2015	Review prior to approval	
V1.0.2	07/12/2015	Final review	
V1.0.3	31/07/2018	Annual Review	

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0.1	05/09/18	James McCahill Loretto Gaughran	Review Document
V1.0.3	6/11/18	Michael Denihan / James McCahill	Review Documents for GDPR compliance

Approval

This document requires the following approvals:

Name	Title	Date
James McCahill	IT Manager	06/11/18
Michael Denihan	Computer Services Manager	06/11/18

This Password Standard shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1 Overview

A poor password management process creates risks to the Institutes information systems and resources. A password standard for the management of passwords will help to mitigate these risks and ensure compliance with GDPR requirements to prevent unauthorised access to Institute's application systems and personal data repositories.

2 Purpose

The purpose of this document is to provide specific guidance to Dundalk Institute of Technology staff and students in relation to passwords. This standard supports the Dundalk Institute of Technology Information Security Policy which should be read in conjunction with this password standard.

3 Definitions

Password – A secret word, pin or phrase that must be used to gain access to a Dundalk Institute of Technology system and/or application which allows for user accountability.

Authentication - Authentication is the process of determining whether someone is, in fact, who they declare to be. Authentication is commonly done through the use of logon passwords.

Privilege Account – A Privilege account has more access than a standard user. These are accounts that are used and maintained by Computer services to manage and maintain the IT infrastructure and services delivered to users on campus.

4 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

End Users	• To ensure their passwords are kept private, changed regularly and not shared with others. • To comply with all Dundalk Institute of Technology Policies and supporting standards and procedures. • Users are forbidden from sharing / using someone else's password to access IT systems. Any breach will result in disciplinary action under the relevant staff / student procedures.
IT Manager	• To ensure compliance with password standard. To inform the management of non-compliance and/or suspected breaches of the password standard.
Application Data Owners	• Ensure application passwords are enforced to the agreed standard. • To inform the SLT of non-compliance and/or suspected breaches of the password standard • Non-compliant applications will be logged in the risk register To report directly on data protection risk (GDPR) and compliance to executive management.
Network Administrator	• Ensure Network systems and servers password standards are enforced to the agreed standard. • To inform the IT Manager of non-compliance and/or suspected breaches of the password standard • Non-compliant network systems will be logged in the risk register

If you have any queries on the contents of this Policy, please contact the Senior Leadership Team or Data Protection Officer.

5 Scope

This standard applies to:

- All users of Dundalk Institute of Technology's information systems and information assets.
- Contractors in respect of the facilities and services that they provide to Dundalk IT

This document also contains specific password rules for the major applications hosted in the EduCampus service platform that users need to be aware of.

Deviations from this policy require authorisation of the IT Manager.

6 Password Standard

- All passwords should be a minimum length of 8 characters.
- Passwords should contain at least:
    - One Upper-case letters
    - One Lower-case letters
    - One Numeric characters
- Passwords can contain Punctuation and Special characters (!"£%^&*@# etc.)
- Password should be hard to guess, thus passwords should not be a word that would be found in a dictionary and passwords should not be based on personal information e.g. family names, birthdays.
- All user-level passwords (e.g. email, web, desktop computer etc.) must be changed every 180 days.
- A Password history of 24 should be maintained
- All administrator passwords must be reviewed/changed every 180 days (this should be a manually enforced password change for those accounts that have service dependencies.
- All privilege account must be reviewed reviewed/changed every 180 days. The standard password aging for these accounts is 180 days.

Where the above standard is not forced by the system or application, Dundalk Institute of Technology users should voluntarily apply this standard to ensure the accounts and passwords cannot be compromised.

6.1 Password Protection

- Passwords should never be written down in hard copy, stored electronically, written in an email or verbally communicated to others.
- Passwords should never be communicated to or shared with other persons.
- Do not use the "Remember Password" function on any applications or web-page.
- For strong robust passwords use phrases etc.

6.2 How to change password

6.2.1 On PC

Use Ctrl-Alt- Del then select Change Password Options

6.2.2 To change Passwords via Web

Step 1-Logon to https://webmail.dkit.ie

Step 2 Select change password facility

Step 3 Enter Old Password

Step 4 Enter new Password twice to confirm new password

6.3 Password Management

Password Reuse:

A password may not be reused within a 12 month period or within 24 instances of a password being changed. Limiting reuse reduces risk by preventing users from repeatedly using the same one, two or three passwords.

6.4 Lost or compromised passwords

Compromised passwords

- Compromised accounts will be disabled until the user presents valid photo id.
- Immediately report to the IT Helpdesk, the loss, theft, or compromise of passwords; and immediately change the password or disable account if user cannot be reached, if compromised.
- Computer Services practice is to adhere to consistent, secure processes for verifying user identity before providing a replacement password.
    1. Present yourself in person to the helpdesk (or local IT technician) With valid /current DkIT id card
    2. Reset password
    3. Validate/re-enter security credentials
    4. Reset password

Forgotten passwords must be reset by presenting yourself on-site to help desk or local technician to get your credentials reset.

6.5 Application Passwords

Many Applications have their own password management systems. These applications can apply many of the rules outlined in the password standard to ensure secure access to the respective applications. See tips for creating strong passwords

6.6 Tips for Creating a Strong Password

- Avoid words, numbers, or known information about you . (e.g. PPSN ; Names, family names, pet names; birthdays, phone numbers, addresses; etc.)
- Avoid using your login name or any variation of your login name as your password. If your login is ‘bloggs’, do not use substitution or letter reordering. Examples would be ‘b10ggs’, where the 0=o and the 1 (one)= l.
- Do not use sggolb (backwards) or add a digit to the beginning or end of the word (1bloggs or bloggs1).
- Avoid using the same character for the entire password (e.g., ‘11111111’) or using fewer than five unique characters.
- Avoid common letter or number patterns in your password (e.g., ‘12345678’ or ‘abcdefgh’).
- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).
- When changing a password, change to an entirely new password. Do not just rotate through a list of favourite passwords.