IT Services
Password Protection Standards

May 2017 v2.1

1. Overview

Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of University College Dublin's resources. All users, including contractors and vendors with access to the University's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

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

3. Scope

The scope of this guide includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides on University network, has access to the University network, stores any non-public University information or has been authorized as a University service including but not limited to public and private cloud services.

4. Password Standards

Password Creation

- Your University password must be unique to University systems. Users must use a separate password for all non-University systems, for example use a different password for websites and applications (including mobile apps) such as LinkedIn, Facebook, social media sites and applications, online shopping accounts, online personal memberships and so on.
- All user-level and system-level passwords must conform to the password construction standards in section 5.
- Where possible, user accounts that have system-level privileges or administration privileges must use a unique password from all other accounts held by that user.

Password Change Frequency

- All user and system level passwords (for example, UCD Connect, computer, application, administrator, root accounts and so on) should be changed at least every twelve months.

Password Protection

- All University passwords are to be treated as sensitive, confidential University information.
- Do not share University passwords with anyone including IT Services, administrative assistants, secretaries, managers, co-workers while on leave, and family members.
- Passwords must not be inserted into email messages or any other forms of electronic communication.
- Do not reveal a password on questionnaires or security forms.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident to the ithelpdesk@ucd.ie and change all related passwords immediately.

5. Password Construction Standards

5.1 Systems will enforce the following passwords characteristics

- Contain at least 8 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).

5.2 Password that have the following characteristics are considered weak:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number, letter or keyboard patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123” “L3tm31n”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use this example as a password!)

6. Related Standards, Policies and Processes

- University Acceptable Usage Policy
- University Cloud Evaluation Guide

Revision History

This guide is regularly reviewed and updated.

Date of Change	Responsible	Summary of Change
Dec 2016	Paul Kennedy	First edition
May 2017	Paul Kennedy	Exec Team changes – 31/5/2017. Moved Appendix to Authentication standards
June 2017	Paul Kennedy	First edition agreed by Exec.