Password Protection Policy

Policy owner	IT Services	**Approval date and body**	October 2018

1. Purpose

Passwords are the most common form of authentication used to control access to information and are an important part of University College Dublin's (UCD) efforts to protect its technology systems and information assets. This policy is designed to address password weaknesses by establishing a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are widely used because they are simple, inexpensive, and convenient mechanisms to use and implement access control. At the same time UCD acknowledges that passwords are recognized as poor form of protection for access control. For some higher-risk systems or for those with access to sensitive data, other approved authentication methods that provide higher levels of trust and accountability should be used where available.

This policy sets out University standards for:

- The creation of strong passwords
- The frequency of change and reuse of those passwords
- The protection of those passwords

2. Definitions

A **"strong"** password is one which has the following characteristics:

- Password is unique.
- Contains at least 10 alphanumeric characters.
    - Password must include at least one letter.
- Includes at least two of the following characteristics
    1. Contains both uppercase and lowercase letters.
    2. Contains at least one number (for example, 0-9).
    3. Contains at least one symbol or special character (for example !$%^&*()_+|~-=\?<>.)

A **"weak"** password is one which has the following characteristics:

- Contains less than 10 characters.
- Can be found in a dictionary, including foreign language, or exist in language slang, dialect, or jargon.
- Has been discovered in a data breach commonly known as a broken password.
- Contains personal information such as birth dates, addresses, sports teams, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contains work-related information such as building names, system commands, sites, companies, hardware or software.
- Contains a number, letter or keyboard pattern such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contains common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Is some version of "Welcome123" "Password123" "Changeme123" "L3tm31n"

3. Scope

All members of UCD’s student, faculty and staff population as well as all contractors and temporary staff 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 the 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. Procedure

Password creation

- All user-level and system-level passwords must conform to standards of a ‘strong’ password.
- All user-level and system-level passwords must not have any of the characteristics of a ‘weak’ password.
- University passwords 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.
- 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 and reuse

- All passwords must be changed if there is thought to be risk to UCD data because:
    - The password does not conform to standards of a ‘strong’ password.
    - There is suspicion that an account has been compromised.
- All staff, visitor, pensioner and system level passwords should be changed at regular intervals, ideally at least every 12 months.
- Passwords cannot be reused.

Password protection for users

- University passwords must be treated as sensitive, confidential University information.
- University passwords must not be shared with anyone including IT Services, administrative assistants, secretaries, managers, co-workers while on leave or family members.
- University passwords must not be inserted into email messages or any other forms of electronic communication.
- University passwords must not be revealed on questionnaires or security forms.
- University passwords should not be written down or stored them anywhere in your office. They must not be stored in a file, on a computer system or mobile devices (phone, tablet) or any electronic format without encryption.
- The "Remember Password" feature of applications should not be used (for example, web browsers).
- University accounts with access to sensitive information should use Multi-Factor Authentication on systems that support it.
- 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.

Password Protection for application owners

- University applications must not store passwords in clear text or in any easily reversible form.
- University applications must not transmit passwords in clear-text over the network.

Password compliance

- The Chief Information Officer or their nominee will have an option of verifying compliance to this policy through various methods, including but not limited to, periodic walk-throughs, system scans and internal and external audits.
- Any exception to the policy must be approved by the Chief Information Officer or their nominee in advance.
- IT Services may withdraw services from any user or system arising from a suspected breach of this policy.

Practical tips for creating a strong password

- Create a password based on a song title, affirmation, or a 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!)
- You should never write down a password. Instead, try to create passwords that you can remember easily.

5. Related Documents

This policy is related to the following existing University policies:

- Acceptable Use Policy
- University Data Protection Policy

The policy will conform to UCD’s responsibilities under Data Protection legislation.

6. Version History

Name	**Version**	**Date**	**Reason for issue**
Paul Kennedy	1.0	Dec 2016	First edition – Password Protection Standards
Paul Kennedy	2.0	Feb 2018	Draft Password Protection Policy
Genevieve Dalton	2.1	Mar 2018	Review by internal IT Services stakeholder group.
Genevieve Dalton	2.2	Jul 2018	Feedback from UMT meeting Apr 2018.
Genevieve Dalton	2.3	Sep 2018	University consultation process.
Phillip Fischer	2.4	Sep 2018	Updated following further consultation.