



Password Policy

TU Dublin Policy on Password Security

Table of Contents

1. Document Control Summary	2
2. Introduction / Context	3
3. Purpose	3
4. Scope.....	3
4.1 Roles and Responsibilities	3
5. Definitions	4
6. Policy Details	5
6.1 Policy Overview	5
6.2 General Standards	5
6.3 Password / Passphrase Requirements	6
6.4 Approval Process	6
6.5 Violation of Policy	6
6.6 Change Process	7
7. Related Documents	7
8. Conclusions	7
9. Appendix	7
10. Document Management	7
10.1 Version Control.....	7
10.2 Document Approval.....	8
10.3 Document Ownership.....	8
10.4 Document Review	8
10.5 Document Storage	8
10.6 Document Classification.....	8

1. Document Control Summary

Area	Document Information
Author	Chief Information Security Officer
Owner	Chief Information Officer
UET Sponsor	Chief Operations Officer
Reference number	TSP2022
Version	1.1
Status	Approved
Pre-approval Body / Bodies	UET, ARC
Approved by	Governing Body
Approval date	1 st December 2022
Next review date	1 st December 2028
Document Classification	TU Dublin Public

2. Introduction / Context

This policy supports the IT regulations to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards, in order to safeguard university systems and data.

3. Purpose

The purpose of this document is to provide specific guidance to users and IT administrators in Technological University Dublin (hereafter referred to as “TU Dublin” or “the University”) on the use of passwords (also known as passphrases) to access University on-line resources. This is because passwords/passphrases are an important aspect of information security, and a poorly chosen password could result in TU Dublin data being lost or stolen. All users, including 3rd-party contractors and visitors with access to the University’s systems, are responsible for taking the appropriate steps to select and secure their passwords.

This **Password Policy** aligns with the following cybersecurity framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Identity Management, Authentication, and Access Control (PR.AA)
 - PR.AA-03

4. Scope

This policy applies to all users who are allocated an account (or any form of access that supports or requires a password) on any system that has access to the TU Dublin network, stores any personal data or private non-personal TU Dublin data, or has been authorised as a TU Dublin service including, but not limited to, external cloud services.

4.1 Roles and Responsibilities

The following roles and responsibilities apply in relation to this policy where appropriate:

Governing Body:

- To review and approve the policy on a periodic basis.

TU Dublin Executive and Management Teams:

- To review and approve the policy on a periodic basis.

TU Dublin Chief Operations Officer:

- To ensure the policy is reviewed and approved by the Executive and Management Teams.

Technology Services Management:

- To clearly communicate information to users on how to create and change secure passwords.
- To liaise with the Office of the University Secretary and/or the University Compliance Group on information received in relation to potential breaches of the policy.

- To enforce compliance with this policy where technically possible on TU Dublin systems.
- To provide tools such as a password-strength meter, or blacklisted words to assist users in choosing a secure password.

Business Data Owners:

- To regularly review the list of accounts with access to business data, and to ensure access is revoked where staff exit their role.
- Review the password policy, and where appropriate, liaise with Technology Services for the configuration of additional security measures

Staff / Students / Third Parties:

- To adhere to the practices contained in this document.
- To report suspected breaches of policy to the IT Service Desk.

For further information on the contents of this policy, please contact [IT Service Desk](#).

5. Definitions

Users: Users are defined as TU Dublin employees, including permanent and temporary staff, students, contractors, sub-contractors, and affiliates with access to TU Dublin IT Resources.

Dictionary Attack: A method of breaking into a user's account by systematically entering every word in a dictionary as a password.

Encryption: The encoding of data so that it cannot be read without the correct decryption key.

Password: A password is a sequence of words or other text used to control access to a computer device, application, or data.

Passphrase is similar to a password in usage, but is longer, and less reliant on complex characters, making it easier to remember. They may also include symbols, numbers, and punctuation marks.

Single Factor Authentication: A process for validating a digital identity using only one set of credentials (e.g., password), in order to gain access to a resource, such as a computer or application

Multi Factor Authentication: A process for validating a digital identity using more than one factor (e.g., a password together with a digital token sent to a mobile phone or physical device/token), in order to gain access to a resource, such as a computer or application.

6. Policy Details

6.1 Policy Overview

This policy states that to protect TU Dublin's systems and data, users must select a password that is secure and difficult to guess.

6.2 General Standards

- The user is the sole custodian of the password and must protect the password at all times.
- Passwords must always be encrypted (non-clear text) when held in storage for any period of time (backup media, batch files, automatic login scripts, software macros, etc.) or when transmitted over networks.
- Passwords must be protected at all times, and measures must be taken to prevent disclosure to any unauthorised person or entity.
- Passwords can be changed using the University's self-service tools. Passwords will only be manually reset by the IT Service Desk when the identity of the user can be verified in person.
- Passwords must not be written down or stored digitally, unless appropriate security measures are in place (e.g., physical security, strong encryption).
- Passwords must not be shared, and Technology Services will never ask users to divulge their password.
- Passwords used to access TU Dublin accounts must not be used for any other applications, sites, or services. This includes non-work related accounts i.e., Twitter, LinkedIn, etc.
- Passwords must be changed immediately when:
 - The password is a default or temporary token created by someone other than the user.
 - A new system is deployed with default vendor passwords.
 - The password is suspected to have been shared or compromised.
- Passwords must never be hardcoded within source code, applications, appliances, or devices.
- Systems and applications must ensure that passwords are not displayed in clear text during the authentication process.
- Staff performing administrative tasks with elevated privileges must use a separate account for this purpose. The username for such accounts should clearly identify the assigned user.
- Any user suspecting that their password may have been breached must report this breach at the earliest opportunity to the IT Service Desk.

6.3 Password / Passphrase Requirements

It should be noted that the requirements outlined in this section should be considered the minimum level of password security that should be applied to TU Dublin passwords.

1. Passwords / Passphrases are a word or string of characters. A strong password should include a minimum of 14 characters (the longer the password, the harder it is for a computer to guess) and must contain one or more of the following:
 - Letters (upper and lower case).
 - Symbols (e.g., &, *, @, €, \$, etc.).
 - Numbers (0 - 9).
 - Punctuation (? ", !).
2. The expiration period for passwords must be set to a maximum of 180 days.
3. The password history setting must be set to remember at least the last 10 passwords.
4. After 10 failed login attempts an account must automatically be disabled for at least 15 minutes or until a system administrator resets it.
5. The initial password issued must be set to expire at first login, requiring the user to choose another password before continuing the login process.
6. Multi factor authentication will be enforced for off-campus access to TU Dublin systems and data.

Exceptions

In circumstances where compliance with some or all of this standard is not practically achievable in the immediate term, an exception must be documented and approved.

This will require completion of an IT Exception Service Request detailing the nature of the exception, and any steps that can be taken to mitigate the resulting risk. This service request shall be approved and retained by Technology Services for the duration of the exception.

6.4 Approval Process

The Chief Information Officer must approve this policy.

6.5 Violation of Policy

Contravention of the policy may lead to the removal of access to TU Dublin resources and may lead to disciplinary action in accordance with the [TU Dublin Staff Disciplinary Procedures](#) or Student Disciplinary Procedures.

6.6 Change Process

This policy will be reviewed every three years or after any change to TU Dublin applications, IT environment or business processes that would affect the implementation of this policy.

7. Related Documents

This policy should be read in conjunction with the following University policies and Users should ensure compliance with all University policies in addition to this policy.

- [TU Dublin Data Protection Policy](#)
- [TU Dublin Acceptable Usage Policy](#)
- [TU Dublin Information Security Policy](#)
- [TU Dublin IT Exception Policy](#)
- [HEAnet Acceptable Usage Policy](#)

The above list is not exhaustive and other [TU Dublin documents](#) may also be relevant.

For further information on IT related queries please contact the [IT Service Desk](#).

8. Conclusions

This policy document will provide a guide to ensure that passwords used to access computer resources are selected and updated in line with best proactive security standards in order to safeguard the university systems and data.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
<i>Draft 1.0</i>	<i>Initial Draft</i>	<i>Richard Dunne</i>	<i>20th January 2022</i>
<i>Ver 1.1</i>	<i>Updated Purpose Section and Document Control</i>	<i>Ronan Dunphy / Preetam Kolekar (ISGRC)</i>	<i>15th January 2025</i>

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
<i>Rev 1.0</i>	<i>17th August 2022</i>	<i>University Executive Team</i>
	<i>2nd November 2022</i>	<i>Audit Risk Committee</i>
	<i>1st December 2022</i>	<i>Governing Body</i>

10.3 Document Ownership

Accountability for defining, developing, monitoring, and updating the contents of this document rests with the Office of the Chief Operations Officer

10.4 Document Review

The Chief Operations Officer is accountable for reviewing this document in consultation with relevant stakeholders. This document should be approved by the Chief Operations Officer, the University Executive Team, and Governing Body.

10.5 Document Storage

This document will be stored on the TU Dublin content management systems under the Policies and Forms media folder / Technology Services sub-folder. The file will be called: "TU-Dublin-Password-Policy-TSPP2022_v1.1.pdf" once released.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to all.