



# Password Policy v1.1

<b>Policy Owner:</b>	Information Security
<b>Creation Date:</b>	27 <sup>th</sup> February 2020
<b>Review Date:</b>	
<b>Version:</b>	1.1
<b>Scope:</b>	This policy applies to all employees and students of Maynooth University
<b>Related Policies:</b>	Information Security Policy

## Revision History

<b>Version</b>	<b>Date</b>	<b>Comment</b>
1.0	13.6.19	Original Release
1.1	27.02.20	Updated following additional consultation

Next Review Date: 2022

## Table of Contents

1	Purpose of the Policy.....	4
2	Scope of the Policy.....	4
3	User Obligations.....	4
4	User Password Management.....	4
5	Review and Reporting.....	5
6	Contact.....	5

## **1 Purpose of the Policy**

The purpose of this policy is to prescribe rules to ensure secure password management and secure use of passwords.

## **2 Scope of the Policy**

This password policy applies to all employees and students of Maynooth University, who have accounts to access Maynooth University computing resources.

## **3 User Obligations**

Users must apply good security practices when selecting and using passwords:

- passwords must not be disclosed to other persons, including management and system administrators
- passwords must not be written down and left in a place where unauthorized person might discover them
- passwords must be changed if there are indications that passwords or the system might be compromised – in that case a security incident must be reported
- passwords must never be shared, regardless of the circumstances. To do so exposes the authorised user to the responsibility for any actions taken using their credentials
- each user may use only their own uniquely allocated username
- users must not construct passwords that are identical or substantially similar to passwords they have previously used
- strong passwords must be selected, in the following way:
  - using at least sixteen characters;
  - passwords must not be based on personal data (e.g. date of birth, address, name of family member, etc.); and
  - passwords used for private purposes must not be used for accessing University IT systems.

## **4 User Password Management**

When allocating and using user passwords, the following rules must be followed:

- each user must have the option to choose their own password, where applicable
- the temporary password used for first system log-on must be unique and strong, as prescribed above
- temporary passwords must be communicated to the user in a secure manner, and user's identity must be previously checked
- the password management system must require the user to select strong passwords
- if the user requests a new password, the password management system must determine the identity of the user by asking identity verification questions
- passwords created by the software or hardware manufacturer must be changed during initial installation

## **5 Review and Reporting**

The policy will be reviewed and updated on, on-going basis, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practices.

## **6 Contact**

Maynooth University Information Security Manager  
Email: [informationsecurity@mu.ie](mailto:informationsecurity@mu.ie)  
Telephone: +353 1 708 6388