DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Password Policy

Purpose

One of the vital components for an organisation to operate a secure and controlled information systems environment is the deployment of approved security mechanisms (e.g., Identification & Authentication, Access Control, Data Integrity and Confidentiality) that support its security services. One of the key mechanisms is the definition and implementation of a uniform 'Password Policy' throughout the organisation.

Accordingly, this policy has been compiled to define the base level password requirements for use within Dublin City University and its wholly owned campus companies (hereinafter collectively referred to as the 'University') and demonstrates its commitment to information security and a proactive approach for addressing risks within the University.

Scope

This policy applies to all accounts used to access the University's Information & Communications Technology (ICT) resources.

This includes all staff, students, suppliers (including contractors) and other third parties (collectively hereinafter referred to as 'Users') who are authorised to access the University's systems and information.

The password requirements defined in this policy apply to all systems that have the facilities to cater for them. Where systems do not have the facilities to cater for the requirements set out in this policy then alternative requirements, on a case-by-case basis, can be implemented with the prior approval of the Director of ISS.

Any deviation from this policy will require prior written approval of the Director of Information Systems Services (ISS).

Policy Statement

This policy is intended to ensure that users are aware of the password requirements that they must adhere to when using the University's ICT resources.

Password Requirements

A) General Requirements

- Multi-factor authentication (MFA) is a critical layer in the University's overall cybersecurity posture and should be implemented, whenever possible.
- All passwords must have at **least fourteen (14) characters.**
    - The length of passwords must always be checked automatically at the time that users construct or select them.
- Passwords should be **easy to remember but hard to guess** so passphrases should be used instead of traditional passwords.
    - Derivatives of user-IDs, and common character sequences such as '123456', must not be used.
    - Likewise, personal details (e.g., spouse's name, vehicle license plate, Personal Public Service Number (PPSN), birthday etc.) must not be used.

  After **five (5) unsuccessful** login attempts, the account must be locked for at least one hour, or until it is reset by a system administrator.
- The initial passwords issued by a security administrator must be valid only for the involved **user's first on-line session**.

B) Management of Passwords

- The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe, or subsequently recover, them.
- All University network devices (e.g., routers, firewalls, access control servers etc.) must have passwords or other access control mechanisms.
- All vendor-supplied default passwords must be changed before any computer or communications system is used for University business operations.
- All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed to unauthorised parties.
- Passwords must not be sent by email or by regular post.
- Passwords must always be encrypted (non-clear text) when held in storage for any period (e.g., as backup media, batch files, automatic login scripts, software macros etc.) or when transmitted over networks.
- Disclosure of incorrect log-in information - when logging into a University computer or data communications system if any part of the log-in sequence is incorrect the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire login process was incorrect.
- To allow passwords to be changed when needed, passwords should not be hard-coded (incorporated) into software developed or modified by University employees or third parties.

C) Password Sharing / Re-use Prohibition

- Computer and communication system access control must be achieved via passwords that are unique to each individual user.
- Users are responsible for all activity performed with their personal user-IDs.
- User-IDs may not be utilised by anyone but the individuals to whom they have been issued.
- Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like 'Guest').
- Users must not use their DCU password on third-party systems or services (e.g., social media platforms, online shopping, personal accounts etc).

Roles and Responsibilities

Users have a responsibility to ensure that their actions comply with both the requirements, and the spirit, of this policy.

Heads of Schools and Units are responsible for pursuing the implementation of this policy in relation to the activities of their departments.

Related Documentation

This policy should be read in conjunction with other ICT policies and guidelines all of which can be found on the University Policies webpage.

Contact

Further clarification on this policy can be sought from the Director of ISS.

Policy Review

This policy will be reviewed and amended as and when necessary.

Version Control

Document Name	Password Policy	
Unit Owner	Information Systems Services (ISS)	
Version Reference	**Version 3.0**	**Reviewed Version**
Approved by	Executive	Director of ISS
Effective Date	18th October 2022	23rd March 2023

End.