Digital Access Control Policy

Introduction

This document sets out the Dublin City University (DCU) policy for controlling access to digital systems and cloud services used within DCU and is an essential element of IT and data governance of the University.

Purpose

This policy is a statement of the digital access controls that must be maintained and monitored to prevent any compromise of the security, confidentiality, integrity and availability of DCU's IT systems.

A key principle of this policy is strict adherence to role-based access control viz. that each user must only be able to access the information or resources necessary to do their job ("least privilege" or "least authority").

Scope

Who does this policy apply to?

This policy applies to all staff of the university, both academic and support, including wholly-owned campus companies and research centres.

What systems does this policy apply to?

This policy applies to all digital systems and cloud services used within DCU to store and process University data including, but not limited to, personal data and confidential business data.

Policy Statement

General

- The access control requirements cover all forms of access to digital systems and cloud services used within DCU to store and process University data including, but not limited to, personal data and confidential business data.

- Compliance with the policy is mandatory.

- Access control must employ the following security principles;

- That each user must only be able to access the information or resources necessary to do their job ("least privilege" or "least authority");

  &

- Segregation of Duties – if a task is deemed sensitive in nature (e.g. fund transfer/approval) then it must require two individuals to perform the task or have appropriate strong controls in place which are signed off at Head of Unit or Director level.

Roles and Responsibilities

The following groups of people will have responsibilities for managing different aspects of this policy.

System Owners

- Overall responsibility for the management of the system and its data.

System Managers

- Implement access requests ensuring that each user must only be able to access the information or resources necessary to do their job ("least privilege" or "least authority").
- Ensure that the information resources are secured according to DCU ICT security policies.
- Regularly review users' permissions.

Line Managers

- Approve access requests ensuring that each user must only be able to access the information or resources necessary to do their job ("least privilege" or "least authority").
- Regularly review their team's permissions.
- In the absence of an automated process, inform system owners of leavers to ensure that leavers' accounts are disabled.

All Staff (as users of digital systems) must

- Know and comply with published policies and procedures.
- Request appropriate permissions through line management.
- Notify line managers when permissions are no longer needed.
- Not share access credentials and, in this regard, take responsibility for all activity under their account.

Related Policies and Legislation

This policy should be read in conjunction with all other relevant existing policies and procedures of Dublin City University and relevant national legislation, including

- Data protection legislation and the General Data Protection Regulation (GDPR)
- Information and Communication Technology Security Policy
- Data Classification Policy
- ICT Compliance Policy
- HEAnet Acceptable Usage Policy

Contacts

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

Policy Review

The Director of Information Systems Services (ISS) will draft necessary changes and have them reviewed and approved by the IS Governance Committee as appropriate. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this Policy should be communicated to the Director of ISS. This policy will be reviewed annually.

Version Control

Document Name	Digital Access Control Policy
Version Reference	V1.0
Owner	ISS
Approved by	Executive
Date	8th Decembr 2020

END