Information Security Policy

Table of Contents

Purpose 2
Scope, Objectives and Definitions 2
  Scope 2
  Objectives 2
  Definitions 3
Policy Statements 3
  Confidentiality 3
  Integrity 5
  Availability 5
Roles & Responsibilities 6
Exceptions 7
Sanctions 8
Related Documentation 9
Contact 9
Policy Review 9
Version Control 9

Purpose

This document defines the Information Security Policy for Dublin City University (DCU). It sets out the principles, responsibilities and minimum requirements necessary to safeguard University information, systems and digital services, and to protect staff, students, researchers, contractors and other third parties who interact with them.

DCU considers information to be a critical institutional asset. Inadequate information security may increase the likelihood of service disruption, data corruption, unauthorised disclosure, regulatory non-compliance, financial loss, reputational damage, and harm to students, staff, research activity and University operations.

This policy establishes the University's high-level information security requirements and must be read alongside related standards, procedures and supporting policies.

Scope, Objectives and Definitions

Scope

This policy applies to:

- all academic and professional units of the University, including subsidiary campus companies and research centres;
- all University information, whether held digitally, physically, or in other forms;
- all University-owned, managed, hosted or connected digital systems, services, devices, networks and accounts;
- all staff and students who have been granted access to University information or related assets;
- all external parties, including contractors, agents, consultants, visitors, partner organisations and service providers, where they access, process, store, manage, support or otherwise interact with University information, systems or services.

For the purposes of this policy, staff, students and external parties within scope may collectively be referred to as "Users". However, additional or different obligations may apply to particular groups including staff, students, digital service providers, researchers, system owners and third parties.

Objectives

The objectives of this policy are:

- to help Users understand their responsibilities in protecting University information, systems and services;
- to support the identification, assessment and appropriate management of information security risks;
- to support the confidentiality, integrity and availability of University information and digital resources;
- to support the prompt and effective detection, reporting, investigation and response to information security incidents;

- to support legal, regulatory, contractual, ethical and policy compliance across teaching, research and professional activities.

Definitions

For the purposes of this policy:

Approved means formally assessed and permitted through the University's designated governance, procurement, information security, data protection and/or technical assurance processes, as applicable.

Authorised means granted permission to access, use, administer or perform a specific action in relation to University information, systems or services through the appropriate University access control or approval process.

University Information means any information created, received, stored, processed, transmitted or otherwise handled by or on behalf of DCU in connection with its teaching, research, administrative, commercial or support activities.

Managed Device means a device configured, monitored or controlled through University-approved technical management arrangements.

Unmanaged Device means a device that is not configured, monitored or controlled through University-approved management arrangements.

System Owner means the person or function with designated responsibility for the business purpose, use, oversight and risk management of a system, service or information asset.

Information Security Incident means any actual or suspected event that may compromise the confidentiality, integrity or availability of University information, systems or services.

Policy Statements

DCU is committed to safeguarding the confidentiality, integrity and availability of University information and digital resources. The University will implement and maintain proportionate physical, technical and organisational measures to protect its information, systems and services against unauthorised access, disclosure, alteration, loss, destruction, disruption or misuse, while supporting compliance with applicable legal, regulatory, contractual and policy obligations.

Confidentiality

All DCU Users must respect the rights of individuals and safeguard University information in accordance with its sensitivity, classification and applicable legal, regulatory, contractual and policy requirements, including the University's data protection, privacy and retention requirements where relevant.

- University information must be stored and processed securely, using appropriate physical, technical and organisational controls.
- University information must be stored only on approved, secure and appropriately protected systems, devices and storage locations.
- Information must be retained only for as long as required and must be securely deleted, destroyed or otherwise disposed of when no longer needed, in accordance with applicable retention requirements.
- In accordance with DCU's *Data Classification & Management Policy*, information classified as Internal, Confidential or Highly Restricted must not be stored, transferred or downloaded to unapproved cloud services, unmanaged devices or unencrypted removable media.
- Information classified as Confidential or Highly Restricted must not be transmitted, shared or stored unless appropriate safeguards are in place to ensure that it is accessible only to authorised recipients.
- Only approved systems and managed devices that meet applicable University security requirements may be permitted to connect to University networks and services, in accordance with applicable University controls.
- Systems and devices may be restricted, isolated or removed from University networks and services where necessary to protect University systems, services and information.
- University digital systems, accounts and resources must be used in accordance with the *Digital Resources Acceptable Usage Policy* and other applicable University policies.
- Users must complete security awareness and related mandatory training when granted access to DCU resources and at regular defined intervals thereafter.
- Failure to complete mandatory information security training may result in proportionate restriction, suspension or withdrawal of access to University digital systems or services, in line with University procedures.
- Mobile devices used to access, process or store University information must be protected through appropriate controls, including device security, password or PIN protection, encryption where appropriate, and automatic locking.
- University information must not be stored on unencrypted removable media.
- Non-University-owned or unmanaged devices may only be used to access, process or store University information where this is expressly permitted through approved University arrangements and where all applicable security requirements are met. Information classified as Confidential or Highly Restricted must not be stored on unmanaged devices unless explicitly authorised and protected through approved compensating controls.
- Any actual or suspected loss, theft, unauthorised disclosure, compromise or misuse involving University information must be reported immediately through the University's designated incident reporting channels.
- Incidents involving personal data must also be escalated and managed in accordance with the University's *Data Privacy Policy*, *Personal Data Retention Policy*, and applicable personal data breach procedures.
- Research data, research systems and research collaborations must be managed in accordance with applicable security, legal, regulatory, contractual, ethical and funder requirements, and in line with the University's *Code of Good Research Practice*, where applicable.
- Approval of new digital systems and cloud services must be obtained in accordance with the *Digital Systems & Cloud Services Policy* before procurement, implementation or use.

The University reserves the right to restrict, suspend, disable or reset access to accounts, devices or services where necessary to protect University information, systems and services from unauthorised access, loss, misuse or compromise.

Integrity

All Users must ensure that University information, systems and services are protected against unauthorised alteration, corruption, loss or destruction, in accordance with applicable legal, regulatory and policy requirements.

- Appropriate controls must be implemented to protect University information from unauthorised alteration, corruption, loss or destruction. Such controls may include secure storage, encryption, access controls, segregation of duties, version control, monitoring and secure configuration.
- Access to create, amend, delete or manage information, and to systems that process or store it, must be restricted to authorised users only and based on least privilege and need to know.
- Access rights must be approved, provisioned, reviewed and withdrawn in accordance with University access control requirements. Access must be limited to what is necessary for the user's role and removed promptly when no longer required.
- Changes to University systems, applications and services must be made only in accordance with approved change management procedures and with due regard to security, resilience and service continuity.
- Users must not disable, alter or bypass security controls where doing so may reduce the security of University systems, services or information.
- The University may monitor, log and review the use of its information, systems, networks, services and digital resources, including network and internet activity where necessary and justified, for defined security, operational, compliance, audit and investigative purposes. Any such activity will be carried out lawfully, proportionately and in accordance with applicable legislation and University policy.
- The University may retain logs of system access, security events, unauthorised access attempts and system changes where required to support monitoring, investigation, audit, incident response, and compliance obligations.
- The University must take reasonable steps to prevent security incidents through appropriate monitoring, vulnerability management and secure configuration of its systems and networks.
- Users must report any actual or suspected information security weakness, vulnerability, threat or incident as soon as they become aware of it, using the University's designated incident reporting channels. Reporting is required for suspected incidents as well as confirmed incidents.
- The University provides out-of-hours arrangements for urgent cybersecurity incidents.

Availability

All DCU Users and digital service providers must support the availability and resilience of University information and digital resources in accordance with applicable legal, regulatory, contractual and policy requirements.

- University information must be backed up regularly using approved University procedures, tools and services, where appropriate to the nature and criticality of the information and service.
- Only approved cloud services must be used for the backup of University information.
- Appropriate protective controls, including anti-malware measures, resilience controls, patching, maintenance and system hardening, must be implemented to reduce the risk of system disruption, data loss, unauthorised access or unauthorised amendment.
- Systems must be maintained through appropriate patching, updates and maintenance activities, with due regard to minimising disruption to service and data availability.
- The University and relevant service providers must maintain appropriate business continuity and disaster recovery arrangements to support the restoration of critical systems, services and information following a disruptive event.
- Critical systems, services and information assets must be identified and supported by appropriate recovery priorities, backup arrangements, restoration procedures and, where relevant, supplier recovery commitments.
- Backup and recovery arrangements must be tested periodically where appropriate, or otherwise supported through appropriate assurance from relevant service providers, to provide confidence that restoration arrangements are effective and aligned to agreed recovery requirements.
- Where critical services are provided through third-party cloud or SaaS arrangements, the University must ensure that appropriate contractual, assurance, escalation and business continuity arrangements are in place, recognising that restoration timeframes may depend in part on provider-operated environments.
- Users must store and back up University information only through approved services and must not rely on local device storage where this creates a risk to availability, integrity or security.
- Where remote working is permitted, appropriate controls must be implemented to protect University information and assets accessed, processed or stored off-site, including physical security measures, secure remote access arrangements, and appropriate local safeguards.

Roles & Responsibilities

Responsibility for implementing this policy is shared across the University and operates through the University's governance, management and operational structures. While Digital Technology Solutions (DTS) is responsible for leading and coordinating the University's information security programme, responsibilities for the secure operation, support and governance of systems and services may also sit with system owners, Heads of Schools and Units, principal investigators, distributed support functions, service providers and other designated roles, depending on the nature of the system, service or activity.

The University's Governing Authority is ultimately responsible for exercising oversight over the University's information security governance arrangements, including significant risks, policies and assurance.

DCU Executive Committee is responsible for approving information security risk management measures, supporting implementation, and ensuring appropriate resourcing, oversight and institutional accountability.

The IS Governance Committee is responsible for maintaining oversight of information security, cybersecurity, digital risk and compliance matters within its remit, reviewing the effectiveness of related policies, procedures, controls and tools, and making recommendations to DCU Executive Committee on relevant policies, significant risks and related matters.

The Director of Digital Technology Solutions has delegated responsibility for implementing, operating and reporting on the University's information security programme. This includes establishing supporting policies, standards and controls, delivering and operating security services, maintaining security monitoring and incident response capability, and reporting significant risks and incidents to the IS Governance Committee, with escalation through other University governance or incident management structures where required.

Heads of Schools and Units are responsible for promoting awareness of this policy and supporting its application within their areas of responsibility. They are also responsible for ensuring that systems used within those areas are appropriately identified, recorded in the University Digital Systems Register, and reviewed and kept up to date as changes occur.

System owners must ensure that systems and services under their authority are appropriately governed, risk assessed, documented and operated in accordance with University requirements. Where systems or services process, store or manage University information, data-related ownership, accountability and decision-making must align with the University's *Data Governance Policy.*

Principal investigators, research leads and relevant owners of research information or systems are responsible for ensuring that research activities under their authority are conducted in accordance with applicable security, legal, regulatory, contractual, ethical and funder requirements.

Third parties who access, process, store, manage or support University information or systems must comply with applicable University information security requirements and any relevant contractual obligations. Appropriate due diligence, contractual controls, onboarding arrangements, assurance requirements, incident notification obligations and exit arrangements must be applied in proportion to the level of risk.

All staff, students and third parties are responsible for using University assets appropriately, complying with this policy and related requirements, completing mandatory training where required, and reporting actual or suspected incidents, weaknesses and risks promptly.

Exceptions

Any exception to this policy must be formally documented, risk assessed, and approved by the relevant system owner or other designated approval authority, in

consultation with Digital Technology Solutions and any other relevant University functions.

Exceptions must be time-bound, recorded, subject to compensating controls where necessary, and reviewed periodically.

Sanctions

The University expects all users to adhere to this policy to ensure a safe, secure, and respectful digital environment for everyone.

The University encourages the prompt reporting of errors, concerns, vulnerabilities and incidents in order to reduce harm and support improvement. Any response to a breach of this policy will take account of the nature of the conduct, including whether it arose from deliberate misconduct, negligence, repeated non-compliance or an honest error that was promptly reported.

Where there are concerns about a potential breach of this policy, the University will review the matter in line with its existing regulations and disciplinary procedures. Any action taken will be proportionate and conducted with fairness and due process.

This may include (but is not limited to):

a) restricting, suspending or withdrawing access to University systems or services where necessary to protect University information or digital resources.
b) engaging the University's student disciplinary process in accordance with the Student Code of Conduct and Discipline.
c) engaging the University's staff disciplinary procedures as outlined in Statute No. 5 of 2010: 'Suspension and Dismissal of Employees'.

The University reserves the right to report breaches to An Garda Síochána where it believes a criminal offence may have been committed.

Breaches of this policy may be reported to:

1. the Director of Digital Technology Solutions (DTS);
2. the Chief Operations Officer;
3. the Vice President for People, Equality, Diversity and Inclusion (for staff);
4. the Vice President for Academic Affairs/Registrar (for students).

Related Documentation

This policy should be read in conjunction with the following:

- Digital Resources Acceptable Usage Policy
- Data Classification & Management Policy
- Digital Access Control Policy
- Digital Systems & Cloud Services Policy
- Password Policy
- Student Code of Conduct and Discipline
- Data Privacy Policy
- Data Governance Policy
- Compliance Policy
- Personal Data Retention Policy
- Digital Identity Retention Policy
- Research Integrity Policy
- Code of Good Research Practice
- Position Statement on the use of Artificial Intelligence tools

Contact

Further queries or clarifications on any aspect of this policy may be directed to the Director of Digital Technology Solutions.

Policy Review

This policy will be reviewed as and when changes are required due to material legal, regulatory, organisational, technological or risk-related change.

Version Control

Policy Name	Information Security Policy	
Unit Owner	Digital Technology Solutions	
Version Reference	**Version 2.0**	**Revised Version**
Approved by	DCU Executive	N/a
Effective Date	14th May 2026	N/a

End.