



Information Security Policy

Table of Contents

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

1. Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance Senior Manager
Owner	Chief Operations Officer
Reference number	TSISP2023
Version and Date	2.0
Status	Approved
Approved by To be approved by	University Executive Team and Governing Body
Approval date	11 th October 2023
Next review date	11 th October 2024
Document Classification	TU Dublin Public

2. Introduction / Context

This policy has been established to safeguard the confidentiality, integrity, and availability of the University's information assets. As a leading academic institution, we recognize the criticality of protecting sensitive data, including research findings, student records, financial information, and intellectual property.

This policy outlines our commitment to maintaining a secure computing environment for all staff, students, and third parties. By adhering to this policy, we aim to mitigate risks associated with unauthorized access, data breaches, malware attacks, and other potential security incidents. The policy's goal is to create a trusted digital ecosystem that upholds the values of confidentiality, integrity, and privacy throughout our University community.

3. Purpose

Technological University Dublin's (hereafter referred to as "TU Dublin" or "the University") information systems underpin all of the University's activities, and are essential to its teaching, learning, research and administrative functions. Security of information must therefore be an integral part of the University's operation and structure to ensure continuity of business, legal compliance and to protect TU Dublin from financial and reputational loss.

The purpose of this document is to set direction for information security management within TU Dublin. The policy sets out the overall approach to information security and provides a security model aimed at:

- Implementing good practices to protect information assets from unauthorized use, disclosure, modification, damage or loss.
- Protecting the work and study environment of staff and students and the good name and reputation of TU Dublin.

The TU Dublin Information Security Policy should be read in conjunction with relevant policies, standards, procedures and guidelines which support the implementation of this policy.

4. Scope

The Information Security Policy is intended to ensure the confidentiality, integrity and availability of TU Dublin information and data assets. This includes, but is not limited to, information and data:

- Stored on electronic media such as IT systems, cloud services, USB keys, hard disks, etc.
- Stored on physical media such as printed out, or handwritten on paper, etc.
- Transmitted across internal and public networks.
- Presented using audio visual media.

This Information Security Policy covers usage of all:

- TU Dublin data.
- TU Dublin resources.

This policy applies to, but is not limited to the following TU Dublin related groups:

- TU Dublin staff.
- TU Dublin students.
- TU Dublin third parties.

4.1 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

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 define and implement standards and procedures which enforce the policy.
- To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures.
- To enforce compliance with this policy where technically possible on TU Dublin systems.

Staff/Students/Third Parties:

- To adhere to policy statements in this document.
- To report suspected breaches of policy to the TU Dublin [IT Service Desk](#).
- If you have any queries on the contents of this policy, please contact the [IT Service Desk](#).

5. Definitions

Confidentiality: Confidentiality restricts information access to authorised users.

Integrity: Integrity protects the accuracy and completeness of information through the controlling of information modifications.

Availability: Availability ensures the information is accessible when needed.

Information Asset: Is defined as anything that has value to an organisation. Information has value and is therefore classified as an asset. Information may refer to data that is processed, but may also encompass unprocessed raw data that is stored on TU Dublin IT infrastructure.

Information Technology (IT) Resource: All IT hardware and software owned or held under license, or otherwise controlled by TU Dublin.

Personal Data: Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by TU Dublin.

Sensitive Personal Data: Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin, political opinions, trade union membership, religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence.

User: Defined as an individual who possesses a recognized TU Dublin identity. A TU Dublin identity refers to the official credentials, affiliations, or recognition associated with Technological University Dublin.

Third Parties: Third Parties are defined as any individual consultant, contractor, subcontractor, vendor, agent not registered as a TU Dublin employee, or student who requires access to specific elements of the IT infrastructure, and/or data stored on that infrastructure.

6. Policy Details:

6.1 Policy Overview

TU Dublin is exposed to several risks arising from the management of Information Security. Failure to manage all or each of the risks identified could result in personal loss to individuals, financial loss to the University and/or damage to TU Dublin's reputation. These risks include, but are not limited to:

- Deliberate or accidental loss, deletion or corruption of information; for example, leaving documents where unauthorised access is possible.
- Theft or accidental unauthorised disclosure of customer or confidential data, for example, emailing sensitive information to unauthorised personnel.
- Inaccurate information/unauthorised amendments to information; for example, accidental updates to information.
- Unavailability of information; for example, information which cannot be accessed for business critical activity.

6.2 Confidentiality

TU Dublin staff, students, and third parties are obligated to respect the rights of individuals and to protect confidential data.

All TU Dublin information is to be treated as confidential unless otherwise indicated. Confidential data must not be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Please refer to [TU Dublin's Data Protection Policy](#) for additional information.

Only data classified as public is permitted to be stored on a personally owned device. Data classified as internal, confidential or restricted must be stored on a TU Dublin managed device or resource.

Internal, confidential or restricted data must not be stored or transferred to a cloud-based service (such as a personal email or cloud storage) where the agreement for using such a service is with an individual rather than directly with TU Dublin.

All information should be stored in a secure manner; this may require physical and logical restrictions. Security controls: include encryption, device management and monitoring, and the use of unique identifiers and passwords which are sufficiently complex where staff, students and third parties operate in accordance with the relevant [TU Dublin Password Policy](#).

All information is considered to be a record held by the University and therefore may be the subject of a Data Subject Request or Freedom of Information access request.

Please see Table 1 (Appendix) below for guidance on the security and storage requirements for the different data classification types.

All storage repositories used for the storage of TU Dublin data should be encrypted where possible.

Data must be purged and securely destroyed once it is no longer required.

In the event of loss or theft of TU Dublin personal or confidential data, this must be reported immediately to the University IT Service Desk and/or DPO, whereupon the appropriate breach management process will take effect. The University reserves the right to remotely wipe the device to protect the data from unauthorised access, as well as disable or reset access to any relevant user accounts.

6.3 Integrity

Access rights to amend information and/or to access systems which process and record this information is restricted to authorised personnel.

System changes should be completed in accordance with the relevant University change management procedure.

An appropriate audit trail including the creation, amendment and deletion of TU Dublin data and/or systems should be kept.

TU Dublin will implement mechanisms to ensure the integrity of data throughout its lifecycle. This may include checksums, digital signatures, or other methods to detect and prevent unauthorized modifications, tampering, or corruption of data.

6.4 Availability

To ensure that TU Dublin data and resources are available when required, the following controls should be employed for users and third parties:

- Define procedures for regular data backups and the process of restoring data in case of accidental deletion, hardware failures, or other incidents.
- Prevent system downtime and/or unauthorised data access and amendment through robust anti-virus and anti-malware protection.
- Regularly perform system maintenance, software updates, and patching activities while minimizing disruption to data availability.

- Engage in Disaster Recovery Planning (DRP) to mitigate against serious events which threaten data/system access.

6.5 Monitoring

TU Dublin reserves the right to monitor all TU Dublin IT resources, information assets, content and data at all times.

TU Dublin reserves the right to log any required TU Dublin data concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

TU Dublin may also log all changes made to TU Dublin systems and applications.

6.6 Violation of Policy

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

6.7 Change Process

This policy will be reviewed annually 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 these policies in addition to this policy:

- [TU Dublin Password Policy](#)
- [TU Dublin Data Protection Policy](#)
- [TU Dublin Acceptable Usage Policy](#)
- [HEAnet Acceptable Usage Policy](#)

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

8. Conclusions

The Information Security Policy serves as a vital framework for ensuring the protection and confidentiality of our valuable information assets. By adhering to this policy, we commit to maintaining a secure computing environment, safeguarding against potential threats, and ensuring the confidentiality, integrity and availability of university data.

9. Appendix

Table 1: TU Dublin Data Classification security and storage

	Data Classification			
	Public	Internal	Restricted	Confidential
Access Controls	<p>May be viewed by all members of the University and the public.</p> <p>No access restrictions.</p>	<p>May be seen by all members of the University but would not normally be available to people outside the University. This data could be released to the public under Freedom of Information legislation.</p>	<p>Accessible only by members of the University (staff or designated third parties) who require it to perform their duties.</p> <p>Authentication/Authorisation required for access.</p>	<p>Accessible only to relevant members of staff or designated third parties due to its potential impact on the University (including financial or reputational damage) or third parties and due to its potential adverse effect on the safety or wellbeing of individuals.</p> <p>Authentication/Authorisation required for access.</p>
Data Storage	<p>Can be stored on any device and placed on the internet.</p> <p>There are no restrictions on printing and copying this data, subject to copyright restrictions.</p>	<p>Should be stored on University network folders or intranet.</p> <p>Should be stored on an encrypted TU Dublin managed device.</p> <p>Cannot be stored on a personal device.</p> <p>Physical copies or copies stored on portable devices should not be left unattended.</p>	<p>Should be stored within the University network in locations with restricted access and appropriate security.</p> <p>Should be stored on an encrypted TU Dublin managed device.</p> <p>Cannot be stored on a personal device.</p> <p>Data should only be printed when there is a legitimate business need.</p> <p>Physical copies or copies stored on portable devices are prohibited from being left unattended.</p> <p>Physical copies are required to be labelled 'Restricted'</p>	<p>Should be held only in restricted areas of the University network and protected with secure credentials.</p> <p>Should be stored on an encrypted TU Dublin managed device.</p> <p>Cannot be stored on a personal device.</p> <p>Prohibited from being stored on a portable media device.</p> <p>Should only be printed when there is a legitimate business need and, when not being referred to, held in locked storage.</p> <p>Physical copies or copies stored on portable devices are prohibited from being left unattended.</p> <p>Physical copies are required to be labelled 'Confidential'</p>

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
Ver 1.0	Approved	CISO	06 th February 2019
Rev 1.1	Revision	ISGRC	10 th March 2022
Rev 1.2	Reorganisation of sections to match approved policy template	ISGRC	25 th May 2023
Rev 1.3	TSMGMT Reviewed	ISGRC	7 th July 2023
Rev 1.4	HR Reviewed	ISGRC	17 th July 2023
Ver 2.0	Final version approved by GB no amendments.	ISGRC	10 th October 2023

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
Rev 1.3	14 th June 2023	University Executive Team
Rev 1.4	19 th September 2023	Audit & Risk Committee
Ver 2.0	10 th October 2023	Governing Body

10.3 Document Ownership

Accountability for defining, developing, monitoring and updating the content 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-Information-Security-Policy-TSISP2023.pdf” once released.

10.6 Document Classification

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