Technological University Dublin

Information Security Policy

Version 1.0

Document Location

http://www.dit.ie/aadlt/ictservices/security/itsecuritypolicies/

Revision History

Date of this revision: 1st January 2019	Date of next review: 1st February 2020

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
Draft Version 0.1	21/6/18	Initial Draft by RICHARD DUNNE	
Draft Version 0.2		Draft for circulation to management team	
Draft Version 0.3	16/10/18	Draft incorporating comments by A.G. and S.K.	
Draft Version 0.4	17/10/18	Draft incorporating comments by DC	
Draft Version 0.5	31/10/18	Draft incorporating comments by ED	
Draft Version 1.0	06/11/18	Document version 1 approval BG, SK, and DC	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Title	Date
TU Dublin Governing Body	06-02-2019

This policy shall be reviewed on an annual basis.

Table of Contents

1. PURPOSE

Technological University Dublin (hereafter referred to as "TU Dublin" and/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.

TU Dublin information security policy should be read in conjunction with relevant standards, procedures and guidelines which support the implementation of this policy (Refer to Section 5).

2. DEFINITIONS

Information Security –The ISO 27002 standard defines information security as the preservation of confidentiality, integrity and availability of information.

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 –The ISO 27002 Standard defines an asset as anything that has a value to an organisation. Information has value, and is classified as an asset. Information refers to data that is processed, but also encompasses unprocessed data that is stored on TU Dublin Information Technology (IT) resources.

Content - Content is information with relevant metadata that has a specific use, or is used for a particular business purpose.

Records – ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Information Technology (IT) Resource – All IT systems owned, held under licence or otherwise controlled by TU Dublin including but without limitation to:

- Workstations including desktop PCs and laptops;
- Servers;

- Network technologies such as routers (WAN, LAN and wireless) and associated media and systems;
- Printers;
- Phones, Smart Phones, tablets and other portable ICT devices;
- USB and all portable memory devices;
- Cloud computing components (hardware, software and infrastructure)
- All other media and devices provided by TU Dublin;
- All other media and devices used to access TU Dublin Information Assets.

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.

Examples of personal data include, but are not limited to:

- Name, email, address, home phone number
- The contents of an individual student file or HR file
- A staff appraisal assessment
- Details about lecture attendance or course work marks
- Notes of personal supervision, including matters of behaviour and discipline.

Personal Devices: These are physical devices, and for the purposes of this policy, on-line services, which TU Dublin staff use for University-related purposes, and which have not been funded or procured by the University. Such devices can include, but are not limited to:

- Desktop and laptop computers, netbooks
- Smartphones, tablets, etc.
- Portable storage devices such as USB memory sticks, removable hard drives, etc.
- Audio visual recording equipment including cameras, dictaphones, etc.
- Cloud-based email, compute, and storage solutions (e.g. Dropbox, Google) based on a contract with an individual rather than the University

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 or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.

Data - For the purposes of this Policy shall mean information which either:

- is Processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be Processed by means of such equipment;
- is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;

- Does not fall within any of the above, but forms part of a Readily Accessible record.

Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.

Data Controller - Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.

Data Processor - Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within TU Dublin which is Processing Personal Data for the University as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor.

It is possible for one organisation or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the University is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.

3. ROLES AND RESPONSIBILITES

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

Governing Body:

- To review and approve the policy on a periodic basis

Registrar:

- To ensure the Policy is reviewed and approved by the Executive.
- To consult as appropriate with other members of the Executive and Management Teams.
- To liaise with Human Resources (HR) or Registrar's Office on information received in relation to potential breaches of the Policy.
- To ensure the appropriate standards and procedures are in place to support the Policy.

CIO / Head of IT Services:

- 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 inform the Secretary / Financial Controller of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

Data Protection Officer

- To lead the data protection compliance and the GDPR risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations.
- To advise on all aspects of data protection and privacy obligations.
- To monitor and review all aspects of compliance with data protection and privacy obligations.
- To act as a representative of data subjects in relation to the processing of their personal data.

To report directly on data protection risk and compliance to executive management.

HR Office and Registrar Office

- To advise relevant management on the invoking of the TU Dublin Disciplinary Procedures when HR or Registrar's Office is informed of a potential breach of the Policy (Refer to Section 7).
- To support and guide managers concerned in managing the Disciplinary Procedures.

Staff/Students/External Parties:

- To adhere to policy statements in this document.
- To report suspected breaches of policy to their manager, School Management or IT Management.

If you have any queries on the contents of this Policy, please contact the CIO / Head of IT Services.

4. SCOPE

This Information Security Policy covers security of:

- TU Dublin Information Assets
- TU Dublin ICT Resources

This policy applies but is not limited to the following, TU Dublin related groups as defined in Section 3.0 of the IT Documentation Framework:

- TU Dublin staff
- TU Dublin students
- TU Dublin external parties.

Based on the definition of Information Security in section 2, this policy outlines key policy statements relating to these areas.

5. SUPPORTING DOCUMENTS

- TU Dublin IT Documentation Framework;
- TU Dublin IT Acceptable Usage Policy;
- HEAnet Acceptable Usage Policy;

- TU Dublin Data Protection Policy.

The above list is not exhaustive and other TU Dublin documents may also be relevant.

6. POLICY

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 our customers, 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 personnel have access to them
- 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 cannot be accessed for business critical activity.

This policy should not be viewed in isolation. Rather, it should be considered as part of a suite of policies and procedures, the most relevant of which are listed in the Document Information section 5. The applicable TU Dublin campus Data Protection Policy should be referenced.

6.1 CONFIDENTIALITY

TU Dublin and all staff, students, and external parties of the TU Dublin community 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. When data is classified as personal (including sensitive personal data) or confidential data, appropriate access and security controls must be applied in transmission and storage. 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

University data that could reasonably be classified as personal data, or sensitive personal data must not be stored on a personally-owned device, unless secured by University approved enterprise solutions Such data must not be stored or transferred to a cloud-based service (such as a personal Google Mail or Dropbox) where the contract for using such a service is with an individual rather than with TU Dublin

Access to information is granted on a need only basis. TU Dublin staff are granted specific access to allow them to carry out their job functions.

All information is stored in a secure manner; this may require physical and logical restrictions. At a minimum, logical security includes the use of unique identifiers and passwords which are sufficiently complex where staff, students and external parties operate in accordance with the relevant TU Dublin campus password standard.

All hardware used for the storage of TU Dublin data is to be purged of data and securely destroyed once it is no longer to be used.

When tapes and other secondary storage devices reach the end of their useful life, they are to be purged of TU Dublin Data and securely destroyed.

In the event of loss or theft of TU Dublin personal or confidential data, this must be reported immediately to the University IT help desk or DPO, whereupon the appropriate breach management process will take effect. In such cases where TU Dublin security software is installed on a personal device, the university reserves the right to remotely locate and wipe the device to protect the its data from unauthorised access

6.2 INTEGRITY

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

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

An appropriate audit trail including database logs of the creation, amendment and deletion of TU Dublin data and/or systems is maintained by TU Dublin. This is particularly important in relation to the following:

- Data including details on staff, students and suppliers;
- Data including inward fee payments, outward supplier payments, and payroll transactions;
- TU Dublin resource usage data.
- TU Dublin data which may reside outside main TU Dublin system(s).1 Please refer to the relevant campus Data Governance Policy

6.3 AVAILABILITY

To ensure that TU Dublin data and resources are available when required, three key layers of control are employed:

- Prevention of data loss through data back-ups
- Prevention of system downtime and/or unauthorised data access and amendment through anti-virus protection (Refer to campus Anti-Virus Scanning and Protection Standard)
- Ability to respond to events which prevent data/system access through Disaster Recovery Planning (DRP)

7. MONITORING

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

[1] This could include data which resides on external systems or data that resides on internal such as Excel Spreadsheets, local desktop databases, etc.

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.

8. 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 disciplinary procedures.