End User Device Security Policy

TU Dublin Policy on End User Device Security

OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Information Security Governance, Risk & Compliance
Owner	Chief Information Officer
UET Sponsor	*Dr Brendan Jennings, Vice President, Research & Innovation*
Reference number	TSEUDSP2025
Version	1.0
Status	Approved
Pre-approval Body/ Bodies	UET, ARC
Approved by	Governing Body
Approval date	15th October 2025
Next review date	15th October 2028
Document Classification	TU Dublin Public

2. Introduction

The End User Device Security Policy outlines a set of rules and guidelines that govern the use and protection of end user devices that access the university's network and data. These devices include laptops, desktops, tablets, smartphones, and any other electronic equipment that can store or transmit information. The purpose of this policy is to ensure that end user devices are used in a secure and responsible manner, and that the confidentiality, integrity, and availability of the university's information assets and IT resources are maintained.

3. Purpose

The purpose of this policy is to set out the requirements for responsible usage of Technological University Dublin (hereafter referred to as ‘TU Dublin’ or ‘the University’) information technology (IT) resources and information assets.

The policy outlines the required security measures for the protection of TU Dublin owned devices and applies to all end user devices that are owned, leased, or otherwise controlled by the university, as well as to any devices that are owned by university employees, students, contractors, or third parties which access, store, process, or transmit university data. This policy aligns with Zero Trust best practices, ensuring that all devices accessing TU Dublin resources are continuously secured, verified and authenticated, regardless of their location, network or ownership.

Devices include but are not limited to:

- Desktops,
- Laptops, notebooks, and hybrid devices
- Tablets
- Mobile phones (e.g. smartphones)
- Any end user device capable of storing TU Dublin data and connecting to the internet or computer network.

This **End User Device Security Policy** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Policy (GV.PO)
    - GV.PO-01
    - GV.PO-02

- Identity Management, Authentication, and Access Control (PR.AA)
    - PR.AA-01
    - PR.AA-03
    - PR.AA-05
    - PR.AA-06
- Data Security (PR.DS)
    - PR.DS-01
    - PR.DS-10
- Platform Security (PR.PS)
    - PR.PS-03
    - PR.PS-05

4. Scope

The End User Device Security Policy is concerned with the secure usage of:

- TU Dublin data and information assets.
- TU Dublin IT resources.
- TU Dublin end user devices.

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 Vice President of Research and Innovation:

- To ensure the policy is reviewed and approved by the Executive and Management Teams.

TU Dublin Chief Information Officer:

- To review and approve the contents of the policy.

Technology Services Management:

- To define and implement standards and procedures which enforce the policy.
- To oversee, in conjunction with data, resource, and device 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 TU Dublin IT Service Desk.

5. Definitions

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 Party: A Third Party is defined as any individual consultant, contractor, subcontractor, vendor, guest, or 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.

End User Device: An end user device (hereafter referred to as a "device") is any electronic hardware that an individual within an organization uses to perform their tasks.

End User Device Owner: For university-owned devices, the device owner is the department or unit that purchased or leased the device. For personally owned devices, the device owner is the individual who owns or possesses the device.

Device User: A staff member, student or third party who has primary responsibility for the device and uses the device to access, store, process, or transmit university data. The device user may or may not be the same as the device owner.

Encryption: The encoding of data so that it cannot be read without the correct decryption key.

Removable Storage Device: Any optical, magnetic or electronic storage device or media, including but not limited to CD, DVD, USB drives (i.e. memory stick/keys), and external/portable hard drives.

Multi Factor Authentication: A process for validating a digital identity using more than one factor (e.g. a password together with a digital token sent to a mobile phone or physical device/token), in order to gain access to a resource, such as a computer or application.

6. Policy Details:

6.1 Policy Overview

This policy sets out the rules and guidelines to ensure that end user device users and owners understand their responsibilities and obligations when using TU Dublin devices, resources or data.

6.2 Policy Details

The following security measures are applicable to all devices accessing TU Dublin resources or data.

6.2.1 Network Security Requirements

- All users require a unique set of credentials to connect to the TU Dublin network and access information assets and IT resources and services.

- Network connectivity includes connecting to a TU Dublin wired network, a TU Dublin wireless network or the Eduroam wireless network.

- Device users should not access restricted or confidential university data on their devices over unsecured wireless networks or public computers.

- Confidential data should not be viewed in public places or accessed via unsecured wireless networks.

- Device users should not connect their devices to unknown or untrusted networks or devices that may pose a security risk.

6.2.2 Remote Access

- Remote access to the university's network must be conducted through secure methods and must comply with the university's remote access policies and best practices.

- Unauthorised remote access tools must not be used to connect to the Universities networks or IT resources.

6.2.3 Data Security

- Access to TU Dublin data is limited based on role-based permissions defined by the data owners and Technology Services and enforced automatically.

- Sensitive data should not be stored on end user devices and users must adhere to the University's Data Protection and Information Security Policies.

- TU Dublin data must not be stored on personal cloud storage services, including but not limited to, Dropbox, Google Drive and iCloud.

- On leaving the university users must ensure that all TU Dublin data is deleted securely from all devices.

- If a device with access to TU Dublin data is lost or stolen, it must be reported to the IT Service Desk immediately.

- Device users must report any actual or suspected data breaches as soon as possible in accordance with university procedures.

- Separate profiles should be used on all end user devices to segregate user data.

6.2.4 End User Behaviour

- TU Dublin devices should only be used for authorized university activities. Personal use of devices should be limited and must not interfere with university operations.

- All device users should log out of finished sessions and all devices should employ a locking screensaver with a timeout inactivity period.

- Device users must exercise caution when opening email attachments or clicking on links in emails, particularly from unknown senders.

- Device users should not leave their devices unattended or exposed to theft or damage. Devices must be stored in a secure location when not in use.

- Device users should screen lock their device sessions when moving away from their device in a shared office or space.

- Device users are required to attend security awareness training in order to be alert and aware of the potential theft of TU Dublin data and devices.

- Device users should not share their passwords or access credentials with anyone else. Passwords should not be written down and/or left somewhere that could be accessed by someone else.

- Attention should be given to the physical security of devices, especially computer systems used to access confidential or sensitive data. Portable devices such as laptops, mobile devices and removable storage devices are particularly vulnerable to theft and loss and should be stored in a secure location when not in use.

- It is the responsibility of any device user to follow all relevant university security protocols when accessing university resources.

- It is imperative that any end user device that is used to conduct TU Dublin business be used appropriately, responsibly, and ethically.

6.2.5 End User Device Security

- End user devices must not have unlicensed or illegal software installed.

- Software updates for the operating systems and applications should be applied automatically.

- Devices users should apply and reboot devices regularly when operating system and application updates are required.

- Rooted or Jailbroken devices are forbidden from accessing TU Dublin resources or data and cannot be connected to TU Dublin networks.

6.3 TU Dublin Owned Device Details

The following security measures are applicable to TU Dublin owned devices accessing TU Dublin resources or data.

6.3.1 Technology Services Remote Support

Remote access software used by Technology Services to establish a connection to a user’s TU Dublin device to troubleshoot and resolve support issues may only be initiated with the user’s permission.

- End users should verify the identity and legitimacy of the remote support provider before granting them access to their devices or university data.

- End users should monitor the remote support session and terminate it if they notice any suspicious or inappropriate activity.

6.3.2 End User Device Logging

- TU Dublin device logs are retained on a centralised logging service and reviewed for anomalous behaviour.

6.3.3 End User Device Management

- All TU Dublin devices must be managed by a TU Dublin managed Enterprise Device Management system.

- Users must return all TU Dublin owned devices for sanitisation or disposal upon leaving the University.

- Users must return all TU Dublin owned devices for sanitisation and disposal when they become obsolete or are replaced by a new device.

- Any TU Dublin device retained by a user after leaving the University will not be supported by TU Dublin.

- A TU Dublin device may be remotely wiped by TU Dublin if:

    - The device is reported as lost or stolen.
    - Employment or association with the University has ceased.
    - A policy or data breach, virus or similar security threat is detected.

6.3.4 End User Device Security

- Access to TU Dublin devices must be protected with a password, PIN, or suitable biometric alternative and comply with the TU Dublin Password Policy.

- TU Dublin devices must have full disk encryption to the specified university standard.

- TU Dublin devices must have a current vendor supported operating system and supported software.

- Device users must not install unauthorised software on TU Dublin owned devices, a request must be made to the IT Service Desk for any additional software requirements.

- Device users must not amend any device security settings configured by TU Dublin.

- TU Dublin devices should have the capability of being wiped remotely.

- TU Dublin devices must have an active, up to date TU Dublin managed anti-virus software installed.

- TU Dublin devices must have a TU Dublin managed firewall software that blocks unauthorized network connections and prevents malicious attacks enabled.

- Device users should not have administrator rights on a TU Dublin device.

- Software deployment should be managed through a TU Dublin Enterprise Device Management system.

- Device users must not install remote access software on TU Dublin owned devices, a request must be made to the IT Service Desk if remote access is required.

- Device users must not share their devices with anyone else unless for work purposes and authorized by their supervisors or Technology Services.

6.4 Non-TU Dublin Owned \ Personal Device Details

The following security measures are applicable to non-TU Dublin owned or personal devices accessing TU Dublin resources or data.

6.4.1 End User Device Security

- Personal devices must comply with the university's security policies and standards.
- Cloud accessible TU Dublin resources and data may be accessed and viewed on a personal device, but they must not be used to store TU Dublin data.
- If a device is required by a staff member to complete work-related tasks an end user device should be supplied by the University. A personal device should not be used.
- The university does not provide support for personal devices. This includes software installation, configuration, and troubleshooting.

6.3 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.

6.4 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.

Users should report any suspected violations of this policy to the TU Dublin IT Service Desk. On receipt of any such notice, (or whereby the University otherwise becomes aware), of any suspected breaches of this procedure or its policies, the University reserves the right to suspend a user's access to the University's services and resources.

Where a valid business case exists exceptions to this policy may be approved by Technology Services in line with the IT Exception Policy.

6.5 Change Process

This policy will be reviewed every three years 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 all University policies in addition to this policy:

- TU Dublin Password Policy
- TU Dublin Data Protection Policy
- TU Dublin Acceptable Usage Policy
- TU Dublin Information Security Policy
- TU Dublin Remote Access Policy
- TU Dublin IT Exception Policy
- TU Dublin Data Classification Policy
- TU Dublin Staff Disciplinary Procedure

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

For further information on IT related queries please contact the TU Dublin IT Service Desk.

8. Conclusions

A device security policy is essential for ensuring the protection of the university's data and devices from unauthorized access and malicious attacks. This policy outlines the roles and responsibilities of the users of TU Dublin devices, resources and data, as well as the minimum security requirements and best practices for device configuration, maintenance, and disposal. By following the policy, the university can reduce the risk of data breaches, cyberattacks, and legal liabilities, and enhance the trust and reputation of the institution.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
0.1	*Initial Draft*	*ISGRC*	*31/10/2024*
0.2	*Draft*	*ISGRC*	*27/03/2025*
0.3	*TSMT Review*	*ISGRC*	*08/05/2025*
0.4	*HEAnet Review*	*ISGRC*	*21/05/2025*
0.5	*Draft*	*ISGRC*	*29/05/2025*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
0.5	*10th June 2025*	*University Executive Team*
0.5	*30th September 2025*	*Audit & Risk Committee*
1.0	*15th October 2025*	*Governing Body*

10.3 Document Ownership

Accountability for defining, developing, monitoring and updating the content of this document rests with the Office of the Vice President of Research and Innovation.

10.4 Document Review

The Chief Information Officer is accountable to review this document in consultation with relevant stakeholders. This document should be approved by both the Vice President of Research and Innovation, 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-End-User-Device-Security-Policy-TSEUDSP2025_v1.0.pdf” once released.

10.6 Document Classification

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