IT Asset Management Policy (Cyber Security and Data Protection)

TU Dublin Policy on the Secure Management of IT Assets

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 Dympna O'Sullivan, Vice President, Research & Innovation*
Reference number	TSITAMP2025
Version	1.0
Status	Approved
Pre-approval Body/Bodies	UET, ARC
Approved by	Governing Body
Approval date	18th February 2026
Next review date	18th February 2029
Document Classification	TU Dublin Public

2. Introduction / Context

Technological University Dublin has a wide variety of IT assets under its control, all of which have specific value and requirements for protection. In order to provide effective information security, it is important that all IT assets are identified and responsibility for their protection is allocated correctly.
These responsibilities include ensuring IT assets are handled and used appropriately throughout their life cycle, returned or disposed of when no longer required, and that appropriate controls are placed upon them in line with their sensitivity and value to the organization.

3. Purpose

This policy sets out the main rules for the management of IT assets and may be supported by more specific procedures which detail how these rules should be implemented.
These controls apply to all systems, people and processes that constitute the organization's information systems, including staff, students and all third parties who have access to Technological University Dublin's IT assets.

This **IT Asset Management Policy (Cyber Security and Data Protection)** aligns with the following cyber security framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- Asset Management (ID.AM)
    - ID.AM-01
    - ID.AM-02
    - ID.AM-04
    - ID.AM-05
    - ID.AM-08
- Identify Management, Authentication, and Access Control (PR.AA):
    - PR.AA-01
- Platform Security (PR.PS):
    - PR.PS-05

4. Scope

This policy applies to all Technological University Dublin (hereafter referred to as 'TU Dublin' or 'the University') IT resource users, including permanent and temporary staff, students, guests, contractors, and third parties who use, access, or otherwise employ, locally or remotely, TU Dublin IT resources or data, whether individually controlled, shared, stand-alone, or networked.

This policy applies to all physical and digital information assets owned, leased, or managed by TU Dublin, including those used by third parties on behalf of the university. This includes but is not limited to:

- Hardware (servers, desktops, laptops, mobile devices, network equipment)
- Software (licensed, custom, SaaS)
- Data (structured and unstructured)
- Cloud-based and virtual assets
- Removable media and backup devices

This policy relates to the management of TU Dublin's IT Assets from a cyber security and data protection perspective only. Financial management of TU Dublin's IT Assets is covered by the TU Dublin Fixed Assets Policy.

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.

Senior Management Teams:
- 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.
- To maintain an asset register for all IT assets owned or managed by the school\function.

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

Asset: Anything that holds value for Technological University Dublin.

Asset Owner: an individual, a role, or an organizational unit responsible for the TU Dublin assigned to them. They are responsible for ensuring information assets are handled and managed appropriately throughout their life cycle.

IT Asset: Any hardware, software, digital information, or technology-related resource owned, leased, licensed or utilised by TU Dublin, including, but not limited to computers, servers, networking equipment, software licenses, mobile devices, data storage systems, and cloud-based services.

IT Asset Management (ITAM): The set of policies, processes, and guidelines implemented to manage, control, and optimize the lifecycle of IT assets within TU Dublin. This includes acquisition, deployment, maintenance, usage, and disposal of IT assets.

Cloud Service Data: Any data, information, or content that is uploaded, created, processed, hosted or managed by TU Dublin within a cloud service environment. This data is owned or controlled by TU Dublin and includes sensitive information such as personal data, academic records, research data, administrative files, and other proprietary information stored or processed on cloud service platforms.

6. Policy Details:

6.1 Policy Overview

The IT Asset Management Policy at TU Dublin establishes a structured approach to managing, protecting, and optimizing the use of the university's IT assets throughout their lifecycle. TU Dublin is committed to managing its IT and information assets throughout their lifecycle in accordance with internationally recognized best practices. All IT assets should be:

- Inventoried and uniquely identified
- Assigned clear ownership
- Protected according to their classification
- Used and maintained responsibly
- Disposed of securely and sustainably

By implementing this policy, TU Dublin aims to safeguard university data, reduce operational risks, and ensure the responsible management of technology resources in alignment with institutional goals. This policy applies to all IT assets owned, leased, or managed by TU Dublin and must be adhered to by all faculty, staff, and students involved in the use or management of these assets.

6.2 Policy Details

6.2.1 IT Asset Inventory

An inventory of IT assets associated with information and information processing facilities within TU Dublin should be maintained and stored in an asset management system. The types of assets to be identified and controlled will include, but not limited to:

- Information
- Cloud Service Data
- Hardware

  - Software
  - Physical
  - Virtual
  - Services

- IT assets may be recorded in more than one location or system.
- The inventory should include all essential attributes: asset ID, type, location, user/owner, classification, acquisition date, supplier and status.
- All new acquisitions, transfers, and disposals must be recorded promptly.
- Each IT asset recorded in the inventory will be assigned an agreed owner who is responsible for:
  - All IT assets under their ownership be included in the inventory
  - An appropriate classification is assigned to the IT assets
  - Access to the IT assets is controlled appropriately
  - IT assets are handled correctly, including their disposal
- The IT asset owner may be an individual, a role, or an organizational unit. Day-to-day operation and maintenance of the IT asset may be delegated by the owner to an administrator.
- Rules for the secure use of the IT assets will be defined by the owner and communicated to those who have access to them.
- IT asset records shall be reviewed and audited regularly.
- Upon leaving the university, all IT assets must be returned to TU Dublin, including the secure removal of university data from all systems including non-TU Dublin owned systems.

6.2.2 Acceptable Use and Access Control

- All users are responsible for using IT assets in accordance with TU Dublin's Acceptable Usage Policy.
- Unauthorized use of IT assets is prohibited.
- Logical and physical access to IT assets must be based on the principle of least privilege and need-to-know.

6.2.3 Asset Handling

- All IT assets must be procured through approved TU Dublin channels.
- Assets should be recorded in the IT asset inventory upon acquisition.
- Users will be assigned IT assets based on role or functional requirements.
- User should be made aware of their responsibilities, including security obligations at onboarding or IT asset handover.
- Transfer of IT assets between departments or campuses should be logged and relevant IT asset inventories updated.

6.2.4 Removable Media and Mobile Devices

- Removable media (USBs, external HDDs) used to store TU Dublin data must be encrypted.
- Mobile IT assets (laptops, phones) must be secured with encryption and strong authentication.

6.2.5 Software Licensing

- Approval of software licence agreements (including End User Licence Agreements) must only be done through approved processes.
- Purchasing documentation (including contracts) relating to software must be retained to show entitlement of usage for compliance purposes.
- Sufficient licenses should be purchased to cover all usage of software requiring a license.

6.2.6 Third-Party Asset Management

- Any third-party handling TU Dublin IT assets must adhere to this policy and applicable contractual obligations.
- IT asset access must be restricted, monitored, and revoked upon contract completion or termination.

6.2.7 Disposal of IT Assets

This section establishes guidelines for the secure and responsible disposal of IT assets to protect sensitive data, ensure regulatory compliance, and promote environmental sustainability.

Asset Decommissioning

- Before disposal, IT assets must be officially decommissioned. This includes verifying the IT asset's status, updating records in the IT asset management system, and removing any organizational tags or identifiers.

Data Sanitization

- All data must be securely removed from IT assets prior to disposal. Approved data sanitization methods include data wiping, degaussing, or physical destruction, based on asset type and data sensitivity.
- Documentation of data sanitization is required to verify completion and compliance with data protection standards.

Environmental and Legal Compliance

- All IT asset disposals must follow applicable environmental laws and standards and minimize environmental impact.
- The university may work with certified disposal vendors to ensure compliance with security, environmental and legal requirements.

Third-Party Disposal Vendors

- Any third-party vendor involved in the disposal process must be vetted and approved. Vendors are required to provide certification of data sanitization and environmentally responsible disposal as outlined in the contractual Data Processing Agreement.
- Confidentiality agreements may be required to ensure data protection during the disposal process.

Documentation and Reporting

- Each IT asset disposed of must be recorded, including its asset ID, date of disposal, data sanitization method, and responsible party.
- Disposal records should be retained to support auditing and compliance needs.

Auditing and Compliance

- Periodic audits of the IT asset disposal process should be conducted to ensure compliance with this policy and relevant regulations.
- Non-compliant disposals will be investigated, and corrective actions taken as needed to maintain policy standards.

6.2.8 Compliance

- TU Dublin may conduct internal audits to ensure asset management compliance.

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 TU Dublin policies may lead to the removal of access to TU Dublin services and resources and may lead to disciplinary action in accordance with the TU Dublin Staff Disciplinary Procedures or Student Disciplinary Procedures if applicable.

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 TU Dublin 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 application 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 IT Exception Policy
- TU Dublin Data Classification Policy
- TU Dublin Fixed Assets Policy

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 IT Service Desk.

8. Conclusions

This policy document will provide a guide for IT Asset Management in TU Dublin and identify the safeguards in place to secure such assets.

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*	*16/06/2025*
0.5	*Draft*	*ISGRC*	*01/07/2025*
0.6	*Clarification of scope.* *Addition of Fixed Assets Policy.*	*ISGRC*	*03/02/2026*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
0.5	*25th November 2025*	*UET*
0.6	*3rd February 2026*	*Audit & Risk Committee*
1.0	*18th February 2026*	*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 for reviewing this document in consultation with relevant stakeholders. This document should be approved by 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-IT-Asset-Management-Policy-TSITAMP2025_v1.0.pdf” once released.

10.6 Document Classification

This document is classified as TU Dublin Public and is available to TU Dublin staff, students and third parties.