Cloud Services Policy

TU Dublin Policy on Cloud Services

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
TU DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Chief Information Security Officer
Owner	Chief Information Officer
UET Sponsor	Chief Operations Officer
Reference number	TSCSP2022
Version	1.1
Status	Approved
Pre-approval Body/ Bodies	UET, ARC
Approved by	Governing Body
Approval date	1st December 2022
Next review date	1st December 2025
Document Classification	TU Dublin Public

2. Introduction / Context

This document sets out the Technological University Dublin (TU Dublin) Policy for evaluating Cloud Services (also known as “Cloud Computing” or “Cloud”).

At present there are four widely accepted service delivery models:

- Infrastructure as a Service (IaaS).
- Software as a Service (SaaS).
- Platform as a Service (PaaS).
- Network as a Service (NaaS).

Cloud services are provided via four deployment models:

- **Private cloud** – where services are provided by an internal provider, i.e., Technology Services
- **Public cloud** – where services are provided by third parties, i.e., external companies or entities, over the public Internet.
- **Managed Service provider**– where services are provided by external company(s) or entity(s) for a specific community of users with common interests. (e.g., EduCampus)
- **Hybrid cloud** – where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public cloud.

It is important that staff are aware of the requirements for procuring and/or using a cloud service that is not managed or controlled by TU Dublin. Staff should also be aware of the restrictions on where confidential data can be transmitted or stored.

3. Purpose

The policy is a statement of TU Dublin's commitment to ensuring that all its legal, ethical and policy compliance requirements, including cybersecurity needs are met in the procurement, evaluation, and use of all cloud services.

This **Cloud Services 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
- Asset Management (ID.AM)
  - ID.AM-04

4. Scope

This Policy applies to all users within the University, including permanent and temporary staff, students, contractors, sub-contractors, third parties and affiliates with access to TU Dublin IT Resources.

4.1 Roles and Responsibilities

The following roles and responsibilities apply in relation to this policy where appropriate:

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 liaise with the Office of the University Secretary and/or The University Compliance Group on information received in relation to potential breaches of the policy.
- To enforce compliance with this policy where technically possible on TU Dublin systems.

Business Data Owners:

- To ensure cloud services are evaluated using the agreed Policy

TU Dublin Staff:

- To adhere to the practices contained in this document.
- To report suspected breaches of policy to the IT Service Desk.

4.2 What data and information does this policy apply to?

This policy applies to all University data and information including, but not limited to, personal data, sensitive personal data (or special categories of personal data) and confidential business data and information as defined in the Data Classification Policy.

All information held in the cloud 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 the Data Classification Policy for guidance on the security and storage requirements for different data classification types.

5. Definitions

Users: Users are defined as TU Dublin employees, including permanent and temporary staff, students, contractors, sub-contractors, and affiliates with access to TU Dublin IT Resources.

Data Owners: A process whereby information/data is assigned an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature.

Cloud computing: At its simplest, cloud computing is a type of computing where both applications and infrastructure capabilities are provided to end users as a service through the Internet. Through cloud computing, entities no longer have to own their own computer hardware, infrastructure, platforms, or applications. By way of an example, software as service (SaaS) application services are cloud computing services.

Data: This covers all data (personal and non-personal) held by the University, on paper or in electronic format, including documents, spreadsheets and other data. It includes data held on systems and databases, produced by systems and data to be uploaded to systems, as well as email content.

Sensitive Personal Data (or Special Category 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; trade union membership; criminal convictions or the alleged commission of an offence.

6. Policy Details:

6.1 Policy Overview

This policy outlines best practices and approval processes for using cloud computing services used by TU Dublin. The steps involved in procuring and evaluating cloud services can be complex and subject to legal, ethical and policy compliance requirements. These requirements, outlined below, must be evaluated, and met prior to using such services. This is essential to ensure that personal, sensitive, and confidential business data and information owned, controlled, or processed by the University, its staff, students, and its agents is protected at all times.

6.2 Approval

Where a cloud service is proposed to host University data or information, appropriate written sign off must be received from the data or information owner / controller and from the Head of School or Administrative unit or their designee. This written sign off should be retained.

6.3 Procurement

The purchasing of all cloud services must comply with relevant university procurement policies and procedures. Those involved in the purchase of cloud services should be cognizant of the risk that purchases by different University departments/faculties of the same cloud service or from the same vendor may inadvertently result in procurement thresholds being breached.

6.4 Data Protection

The General Data Protection Regulation (GDPR), and related legislation, requires that Data Controllers such as TU Dublin meet significant obligations regarding how personal data is collected and processed. Consideration should be given for the requirement for a Data Protection Impact Assessment (DPIA) in addition to a comprehensive Data Processing Agreement (DPA). Contact the University's Information Governance Office for more information (dataprotection@tudublin.ie).

6.5 Allowed Hosting of Data

The cloud service proposed must be suitable for the type of data it is intended to store. Please see Table 1 below which will outline the criteria for each data classification type.

Table 1 Data and information matrix for cloud models

Data / Information Classification	Cloud service models for data storage		
	Internally hosted, Managed Service Provider, Private Cloud	Secure Public Cloud	Public Cloud without a guarantee of security and privacy
Confidential	Yes	No	No
Internal	Yes	Yes	No
Public	Yes	Yes	Yes

6.6 System / Service Security

Cloud service providers are required to complete an appropriate assessment questionnaire or tool, which will be provided by Technology Services. Technology Services will undertake a review of this assessment to measure the security posture of the cloud vendor.
Use of a third-party cloud service cannot commence until this assessment process has been completed by Technology Services and any risks are either mitigated or accepted.

6.7 Interoperability

The University is committed to the principles of integration and interoperability of all systems. These principles must be considered and documented as part of any service evaluation. Technology Services must be consulted at the evaluation stage for advice where data from a proposed cloud service is required to integrate with a university system.

6.8 Disaster Recovery / Business Continuity

The service must be selected to ensure that the data and information is secure at all times and that an adequate backup and disaster recovery plan is in place to ensure that data and information can be retrieved in a timely manner.

6.9 Vendor Management and Governance

All new and existing vendors of cloud services should be subject to ongoing assessments in the areas of contract, financial, performance, relationship, and risk management.

6.10 Exit Strategy

Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service. The University must determine how data would be recovered from the vendor and have an agreed retention schedule for any data stored.

6.11 Violation of Policy

Contravention of the policy may lead to the removal of access to TU Dublin resources and may lead to disciplinary action in accordance with the TU Dublin Staff Disciplinary Procedures or Student Disciplinary Procedures.

6.12 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 Data Protection Policy
- TU Dublin Data Classification Policy
- TU Dublin Information Security 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 to TU Dublin for evaluating Cloud Services.

9. Appendix

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
Draft 1.0	*Initial Draft*	*Richard Dunne / Alan Pike*	*27th July 2022*
1.1	*Updated Purpose section and Document Control.*	*Ronan Dunphy / Preetam Kolekar (ISGRC)*	*15th January 2025*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
Rev 1.0	*21st September 2022*	*University Executive Team*
	2nd November 2022	*Audit Risk Committee*
	1st December 2022	*Governing Body*

10.3 Document Ownership

Accountability for defining, developing, monitoring, and updating the contents 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-Cloud-Services-Policy-TSCSP2022_v1.1.pdf” once released.

10.6 Document Classification

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