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	Richard Dunne
Owner	Bridget Gleeson, Head of Technology Services
Reference number	TSCSP2022
Version	1.0
Status	Approved
Approved by	University Executive Team & Governing Body
Approval date	1st December 2022
Next review date	1st December 2023
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.

4. Scope

4.1 Roles and Responsibilities

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

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 Head of Technology Services.

.

4.2 Who does this policy apply to?

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

4.3 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 Table 1 below for guidance on the security and storage requirements for the different data classification types as outlined in the Data Classification Policy.

Please see the Data Classification Policy for additional information relating to these classification types.

Table 1: TU Dublin Data Classification security and storage

	Data Classification			
	Public	**Internal**	**Restricted**	**Confidential**
Access Controls	May be viewed by all members of the University and the public. No access restrictions.	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.	Accessible only by members of the University (staff or designated third party) who require it to perform their duty. Authentication/Authorisation required for access. Refer to the TU Dublin Information Security Policy and Password Policy for guidelines on security of data.	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. Authentication/Authorisation required for access.
Security and Storage (refer to Information Security Policy for appropriate security measures.)	Can be stored on any device and placed on the internet. There are no restrictions on printing and copying this data, subject to copyright restrictions.	Should be stored on university network folders or intranet. Caution should be exercised if data is transferred to any non-TU Dublin TS managed external or mobile devices. See TU Dublin Information Security Policy. Physical copies or copies stored on portable devices should not be left unattended.	Electronic data should be stored within the University network in locations with restricted access and appropriate security. Data should not generally be transferred to external or mobile devices but if essential then appropriate security e.g., encryption must be used. Data should only be printed when there is a legitimate business need. Physical copies or copies stored on portable devices are prohibited from being left unattended. Physical copies are required to be labelled ‘Restricted’	Electronic data should be held only in restricted areas of the University network and protected with secure credentials. Electronic data is prohibited from being stored on a workstation or mobile device, unless the device is fully encrypted. Electronic data is prohibited from being permanently stored on a portable media device (e.g., USB drive). Data should only be printed when there is a legitimate business need and, when not being referred to, held in locked storage. Physical copies or copies stored on portable devices are prohibited from being left unattended. Physical copies are required to be labelled ‘Confidential’

5. Definitions

The following are core definitions used in this document. These include:

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 2 below which will outline the criteria for each data classification type.

Table 2 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
Restricted	Yes	Yes	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. An example of an Assessment Tool is the Educause Higher Education Cloud Vendor Assessment Tool (HECVAT)
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.

7. Related Documents

The following documents relate to the Cloud Services Policy.

- TU Dublin Data Protection Policy
- TU Dublin Data Classification Policy
- TU Dublin IT Security Policy

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

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*

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

This document is owned by the Head of Technology Services, on behalf of the University.

10.4 Document Review

This document must be reviewed annually or after any significant change by TU Dublin.
This document should be approved by both the Chief Operations Officer and the University Executive Team.

10.5 Document Storage

This document will be available for viewer access on the TU Dublin website.

The Head of Technology Services, as owner of the document, will keep the original version, for document control purposes and to meet document retention policy requirements.

10.6 Document Classification

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