Third Party Access Policy

TU Dublin Policy on Third Party Access

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Chief Information Security Officer
Owner	Chief Information Officer
UET Sponsor	Chief Operations Office
Reference number	TSTPA2022
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 policy has been created to outline the minimum-security requirements that third parties accessing TU Dublin systems and information systems must adhere to, to safeguard University systems and data.

3. Purpose

This policy describes the minimum level of security controls that must be in place prior to allowing third party remote access to the TU Dublin IT infrastructure and data.

It is important to note that TU Dublin could suffer reputational, legal, or financial consequences in the event of an information security incident.

This **Third Party Access Policy** aligns with the following framework and controls:

National Institute of Standards and Technology Cybersecurity Framework 2.0

- ○ Cybersecurity Supply Chain Risk Management (GV.SC)
  - GV.SC-01
  - GV.SC-02
  - GV.SC-03
- ○ Identity Management, Authentication, and Access Control (PR.AA)
  - PR.AA-01

4. Scope

This Third Party Access Policy is intended to cover all situations where a third party is providing goods or services in support of the University’s IT infrastructure, which may require them to have access to data that could reasonably be defined in the University’s Data Protection Policy as being private non-personal data, personal data, or sensitive personal data.

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 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.

TU Dublin Data Owners

- To ensure that appropriate contracts and agreements are in place, and to schedule formal periodic reviews of third party compliance with this policy.

Third Party suppliers requiring access to TU Dublin infrastructure and/or University data

- To ensure they are familiar with the contents of this policy, before signing a third-party access agreement with TU Dublin.

- To ensure compliance with this and all relevant supporting TU Dublin Policies and procedures.

Technology Services

- To assist TU Dublin business data owners in ensuring that appropriate oversight is in place with relevant third parties.

- To ensure that the security of the IT infrastructure is not compromised as a direct result of providing access to a third party.

- To ensure all centrally managed IT systems are appropriately updated with the latest security patches.

5. Definitions

Third Parties: Third Parties are defined as any individual consultant, contractor, subcontractor, vendor, or agent not registered as a TU Dublin employee, or student but who will require access to specific elements of the IT infrastructure, and/or data stored on that infrastructure.

Third Party access: Third party access is defined as all physical or remote access to the TU Dublin IT infrastructure for the express purpose of providing goods or services to the University.

TU Dublin network: The TU Dublin network includes all data, applications, systems, services, infrastructure, and computer devices which are owned, leased, or hosted by TU Dublin and are physically located on the TU Dublin campus.

Mobile computer devices: Mobile computer devices are defined as any handheld computer device, including but not limited to laptops, notebooks, tablet computers, smartphone devices.

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

6. Policy Details:

6.1 Policy Overview

This policy states the third party access requirements that must be adhered to, in order to ensure the confidentiality, integrity, and availability of TU Dublin IT resources.

6.2 Policy Details

- A Third Party IT Access agreement must be signed by an authorised representative of the third party, and a Technology Services manager. Such an agreement must include details on:
  - The parties to the agreement.
  - The effective start and end dates for the service being provided.
  - The functions/services being provided.
  - The right of TU Dublin to monitor all access to and use of TU Dublin infrastructure and data, and to audit the compliance of the third party with this policy.
  - The primary contractor and relevant sub-contractors.

- Third parties with access to sensitive TU Dublin data are required to sign a confidentiality agreement to protect University data that they may have direct or indirect access to.

- Third party access to TU Dublin information resources must be approved by the Data Owner and Technology Services.

- Third party access may only be used for the business purposes that it has been granted for. (i.e., service ticket, project, etc.).

- Third party remote access to the TU Dublin infrastructure must use a Technology Services approved method of remote access.

- All third party remote access connections must use Multi Factor Authentication.

- Third parties are responsible for ensuring that only nominated employees have access to the TU Dublin network and for updating TU Dublin in writing of any relevant staff changes at the earliest opportunity.

- All third party access must be uniquely identifiable, and passwords used must comply with the TU Dublin Password Policy.

- Usernames, passwords, and any other credentials used for third party access must not be shared.

- TU Dublin data must not be copied, divulged, or distributed by third parties without the prior written approval of TU Dublin.

- TU Dublin data must never be updated by third parties without the express permission of the relevant TU Dublin data owner, and a record must be made of all such changes.

- All changes that could impact service delivery to the University must obtain prior approval in accordance with the Technology Services Change Advisory Board, Technology Services will coordinate the submission of any change requests.

- Access to a University system will only be provided for the minimal period necessary, and with the minimum level of access required to complete the task. Access will never be left open indefinitely and will be closed without notice following the agreed period.

- For security reasons, all third-party remote access accounts, except those providing 24*7 support, will be disabled by default. Third parties will be required to contact the IT Service Desk requesting that their account be enabled for a stipulated period.

- Third party remote access accounts providing 24*7 support will always remain open for diagnostic purposes. However, third parties will be required to email the IT Service Desk each time the account is used.

- A log of all remote access is retained for audit purposes.

- All requests for amendments to third party access privileges must be formally approved by the data owners and Technology Services.

- All third-party access is subject to a quarterly user access review.

- Where third parties are connecting to the TU Dublin infrastructure from a remote location, they must ensure appropriate physical, and IT based security measures are in place. This will include physical locks, automated key cards, visitor registration, and access logging.

- Third parties must have appropriate information security policies and practices in place, and ensure any devices used to access TU Dublin infrastructure or data are fully up to date with virus protection, personal firewalls, and security updates.

- While onsite third parties must comply with all relevant TU Dublin physical access controls, rules, and regulations.

- Third parties must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any TU Dublin information systems, applications, or equipment. The third party will be held responsible for all disruptions and damage caused to the TU Dublin network, information systems, applications or equipment which is traced back to infected software installed by the third party.

- Third parties must ensure that computer devices connected to the TU Dublin network are not connected to any other network at the same time, with the exception of networks that are under the complete control of the third party. i.e., the use of split tunneling, dual homing or otherwise rerouting TU Dublin traffic is not permitted.

- The issuing of remote access credentials must be done in a secure fashion, using encryption tools such as https://filesender.heanet.ie/and never in an unencrypted form, such as in an email or text message.

- Under no circumstances should TU Dublin data be stored on mobile devices, in personal backups or on removable storage devices i.e., USB memory sticks by third parties.

- Third parties must inform Technology Services at TU Dublin immediately of any suspected or actual data breaches.

- In the event of a suspected data breach, the University's process for managing such incidents will apply. All parties will assist with any investigation as appropriate.

- Off boarding processes and procedures must be in place to ensure that third party access is revoked at the end of the partnership and that acceptable methods for the return, destruction, or disposal of any TU Dublin data in the third party's possession is defined.

- Third parties will be held responsible for all activities performed on the TU Dublin network while logged in under their assigned usernames and passwords.

- All relevant TU Dublin supporting policies, procedures, data protection, legal and regulatory requirements must be compiled with.

Monitoring

The TU Dublin reserves the right to:

- Monitor all third party activity while connected (local and remote) to the TU Dublin network.

- Audit contractual responsibilities or have those audits carried out by a TU Dublin approved third party.

- Revoke the third parties access privileges at any time.

Exceptions

Where a valid business case exists an exception to this policy can be applied for in line with the IT Exception Policy.

6.3 Approval process

Third Party remote access to the TU Dublin infrastructure must be approved by Technology Services in advance and must be for a specified and legitimate purpose. A request form must be filled in by the requester and signed off by the relevant TS manager.

6.4 Violation of Policy

Contravention of the policy by Third Parties 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.

6.5 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 Information Security Policy
- TU Dublin Password Policy
- TU Dublin Acceptable Use Policy
- TU Dublin IT Exception Policy
- TU Dublin Data Protection 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 Third Party access to the TU Dublin network and the safeguards in place to control such access.

9. Appendix

Please see Third Party Access Agreement.

TU DUBLIN THIRD PARTY ACCESS AGREEMENT

The purpose of this agreement is to outline the specific terms and conditions governing access to, and use of, the TU Dublin ICT infrastructure by a third party. This agreement should be read in conjunction with TU Dublin IT security policies, including the **Third Party Access Policy**, and all parties should ensure compliance with these policies.

This agreement, made between TU Dublin and the Third Party listed below, shall take effect on

______________________________and shall expire on_.____________________________________

Signed for and on behalf of TU Dublin	Signed for and on behalf of third party
______________________________	______________________________
being a duly authorised officer	being a duly authorised officer
Date	Date
______________________________	______________________________
Name in block letters	Name in block letters

____

Description of ICT access required by the third party

10. Document Management

10.1 Version Control

VERSION NUMBER	VERSION DESCRIPTION / CHANGES MADE	AUTHOR	DATE
Draft 1.0	*Initial Draft*	*Richard Dunne*	*20th January 2022*
Ver 1.1	*Updated Document Control and Purpose Section*	*Ronan Dunphy / Preetam Kolekar (ISGRC)*	*15th January 2025*

10.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
Rev 1.0	*17th August 2022*	*University Executive Team*
	2nd November 2022	*Audit Risk Committee*
	1st December 2022	*Governing Body*

10.3 Document Ownership

Accountability to defining, developing, monitoring and updating the content of this document rests with the Office of the Chief Operations Officer.

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 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-Third-Party-Policy-TSTPA2022_v1.1.pdf” once released.

10.6 Document Classification

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