Remote Access Policy

TU Dublin Policy on Remote 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	TSRA2022
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 assist staff, students, affiliates, and contractors of TU Dublin in understanding the importance of protecting University data that is remotely accessible via the IT infrastructure.

3. Purpose

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

It is important to note that TU Dublin could be liable to substantial fines and/or compensation claims should it fail to comply with the requirements of GDPR in the protection of personal data.

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

National Institute of Standards and Technology Cybersecurity Framework 2.0
  - o Identity Management, Authentication, and Access Control (PR.AA)
    - PR.AA-01
    - PR.AA-05

4. Scope

This policy applies to all TU Dublin staff, students, affiliates and contractors authorised to use remote access to connect to the TU Dublin IT infrastructure for the purposes of supporting the University's objectives.

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 access controls commensurate with the classification of data are in place for the data they are responsible for.

- To approve requests for remote access and to conduct periodic user access reviews of all users with remote access privileges.

Technology Services

- To assist TU Dublin business data owners in ensuring appropriate oversight is in place.

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

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

Remote access: Remote Access is defined as access to the TU Dublin IT infrastructure from any non-campus network, or from the Internet whether on or off campus.

Users: Users are defined as TU Dublin employees, including permanent and temporary staff, contractors, students, affiliates, Governing Body members and Committee members with remote access to TU Dublin IT Resources.

Third Parties: Third Parties are defined as any individual consultant, contractor, 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.

Malware: Malware or malicious software is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware.

Generic Accounts: Generic Accounts are defined as accounts that are used by a system, application, or service; actions carried out by these accounts are not attributable to individual users.

6. Policy Details

6.1 Policy Overview

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

6.2 Policy Details

- Remote access to the TU Dublin infrastructure must be approved by the relevant Head of Function in advance and must be for a specified and legitimate purpose.

- Remote access must only be used for the purpose of supporting TU Dublin's function and objectives.

- Remote access to the TU Dublin infrastructure must use a Technology Services approved remote access technology.

- All remote access connections must use Multi Factor Authentication where available.

- Users must not install remote access software on TU Dublin owned devices without prior approval from Technology Services. Unauthorised remote access software will be removed.
- When working remotely all applicable TU Dublin policies, and in particular IT security policies, must be complied with.

- All individuals are responsible for safeguarding the remote access credentials granted to them. These credentials may consist of username and password combinations, digital certificates or other software or hardware.

- All individuals granted remote access to TU Dublin systems must comply with the following measures:

    o Use a strong password that conforms to the TU Dublin Password Policy.

    o Users must not provide their password to any other person or entity or attempt to use any other individual's credentials to gain access to TU Dublin resources.

    o Devices used for remote access must have sufficient protection in terms of antivirus, malware protection and operating system patches.

    o Users are required to ensure that the network they are connecting from is secure. Avoid the use spurious free wireless networks to access TU Dublin systems.

- Generic accounts must not be used for remote access.

- Remote workers authorised to access TU Dublin data must take all reasonable steps to maintain the confidentiality of this data when working in public.

- Remote users must only remain connected for as long as required to carry out their work and must disconnect as soon as their work is completed.

- Remote users are advised to save their work at regular intervals.

- Users 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 their complete control. i.e., the use of split tunneling, dual homing or otherwise rerouting TU Dublin traffic is not permitted.

- Remote access users must not download, transfer, or otherwise store TU Dublin information outside of managed applications on mobile devices.

- All remote access is subject to the TU Dublin IT security user access review process.

- Remote users must not attempt to bypass any security measures put in place by the TU Dublin Technology Services team.

- When remote access is provided to any system, access shall be granted on the principle of "least-privilege." Specifically, users shall not be granted access to systems or functions to which they do not need access.

- If any device used for remote access is lost, stolen, or otherwise removed from the user's control, the authorised user will be responsible for notifying Technology Services and their Line Manager immediately.

- Any suspected or actual security incidents involving data should be reported immediately to Technology Services.

- 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.

- All TU Dublin staff, students, affiliates and contractors will be held responsible for all remote activities performed on the TU Dublin network while logged in under their assigned usernames and passwords.

Remote Support

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

It is the user's responsibility to close any windows that may contain private / sensitive information before accepting a remote connection.

Third Parties

Third Parties may be granted remote access on a case-by-case basis, please see Third Party Remote Access Policy.

Logging

Remote access server logs are retained on a central logging server and reviewed for anomalous behavior.

Monitoring

Any device connecting to the TU Dublin IT infrastructure may be subject to monitoring, this may include but is not limited to date, time duration, identification of device and network traffic.

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

Remote access to the TU Dublin infrastructure must be approved by the relevant Head of Function in advance and must be for a specified and legitimate purpose. A request form must be completed by the requester and signed off by the relevant Head of Function.

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 IT Acceptable Use Policy

- TU Dublin Third Party Access 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 provides a guide for Remote Access to the TU Dublin network and the safeguards in place to control such access.

9. Appendix

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	Purpose Section Updated 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	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-Remote-Access-Policy-TSRA2022_v1.1.pdf" once released.

10.6 Document Classification

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