Remote Access Policy

TU Dublin Policy on Remote Access

Table of Contents

1. Document Control Summary 2
2. Introduction / Context 3
3. Purpose 3
4. Scope 3
4.1 Roles and Responsibilities 3
5. Definitions 4
6. Policy Details 4
6.1 Policy Overview 4
6.2 Policy Details 4
6.3 Approval process 6
6.4 Change Process 6
7. Related Documents 7
8. Conclusions 7
9. Appendix 7
10. Document Management 7
10.1 Version Control 7
10.2 Document Approval 7
10.3 Document Ownership 7
10.4 Document Review 7
10.5 Document Storage 8
10.6 Document Classification 8

1. Document Control Summary

Area	Document Information
Author	Richard Dunne
Owner	Bridget Gleeson, Head of Technology Services
Reference number	TSRA2022
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 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.

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 key responsibilities in connection with this policy are as follows:

Users

- To comply with this and all supporting TU Dublin Policies.

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.

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 purposes 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:

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

  - 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.

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

  - 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 may 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.

Compliance with policy

Non-compliance with this policy may lead to the withdrawal of TU Dublin network and remote access privileges and further disciplinary action in accordance with the University's disciplinary procedures.

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 for a period of 180 days 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 exceptions to this policy may be signed off by the Head of Technology Services.

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 filled in by the requester and signed off by the relevant Head of Function.

6.4 Change Process

This policy will be reviewed annually or after any significant change to the TU Dublin infrastructure.

7. Related Documents

This policy should be read in conjunction with the following University policies and Users should ensure compliance with these policies in addition to this policy.

- TU Dublin Information Security Policy
- TU Dublin Password Policy
- TU Dublin Acceptable Use Policy

8. Conclusions

This policy document will provide 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*

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

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

10.4 Document Review

This document must be reviewed at least every year by Technology Services.

10.5 Document Storage

This document will be stored on the TU Dublin public website.

10.6 Document Classification

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