Remote Access Standards

Owner	IT Services	Date Approved	11 Jan 2023

1. Purpose

The purpose of this Remote Access Standards document is to define standards for minimising security risks that may result from unauthorized remote access to the University's IT Resources.

The Remote Access Standards are supplemented by the University's IT Acceptable Use Policy.

2. Definitions

- **IT Resources** includes, but not limited to, University applications, backend servers, infrastructure equipment, databases, industrial control systems, networking equipment, network attached storage, research equipment, IOT (Internet of Things) devices, etc.

3. Scope

These standards apply to university faculty, staff, researchers, visitors or external suppliers when remotely accessing UCD's IT Resources or personal or confidential University information on an untrusted network.

4. Standards

When remotely accessing the University's IT Resources you must ensure that the following measures are taken:

- Remote access to the University IT Resources must use UCD's Virtual Private Network (VPN) solution or a previously approved remote access technology. All other remote access technologies are prohibited, including remote desktop technologies or software which establishes outbound connections to third party sites which can then be used to access a user's desktop remotely.
- Users should use UCD's VPN when accessing or processing personal or confidential University information on untrusted networks e.g. Airport Wi-Fi, Conference Centre Wi-Fi, Hotel Wi-Fi, etc.
- UCD's VPN solution must only be used for University related purposes. Use of UCD's VPN for personal use such as streaming is prohibited.
- You must not attempt to log on to UCD's VPN using another individual's credentials.

- Remote access to end user desktop equipment, including laptops, desktop computers, printers, scanners, etc. is prohibited.
- All devices used for remotely accessing University IT Resources must be protected in line with UCD's Device Protection Policy.
- Individuals wishing to implement alternative remote access technologies must obtain prior permission from IT Services. Requests for alternative remote access solutions should be sent to the IT Service Support Hub https://www.ucd.ie/ithelp.

5. Related Standards, Policies and Procedures

- University Acceptable Use Policy
- University Device Protection Policy
- University Password Protection Policy
- Search IT Support Hub for details of how to request access to UCD Staff VPN
- Search IT Support Hub for details of how to request access to UCD Research VPN

6. Version History

Name	Version	Date	Reason for change
IT Security	V1.5	May 2017	Original publication - document was entitled "Remote Access Procedures".
Paul Kennedy	v2.0	Feb 2023	Approved by ITLG