IT Services
Remote Access Procedure

May 2017 v1.4

1. Introduction

University College Dublin provides information technology services for the University in support of its mission. Remote access to the University's systems by account holders is a requirement to support the University's mission and must be controlled to ensure the confidentiality, integrity and availability of University systems and information.

This procedure outlines the circumstances in which an account holder may gain remote access to systems which are only accessible on the University's network. These procedures are designed to minimize the potential exposure from damages which may result from the unauthorised use of University resources, including the loss of sensitive or confidential data, theft of intellectual property, system availability, reputational damage or corruption of critical systems or data. The Remote Access Procedure are supplemented (and may be amended) by the University's Acceptable Use Policy.

2. Definitions

- The "Account Holder" is an authorised member of the staff, student, visitor or contractor.
- The "Approver" is a member of IT Services senior management team.
- "Systems" are any network registered server or IT Service's supported service that is only available on the University campus network.

3. Requirements

Remote access to the University campus network, systems, and/or data are subject to University policies including but not limited to the University's Acceptable Use Policy, Data Protection Policy, vendor contracts, etc.

Remote access to University Systems must be for a specified and legitimate purpose and must use IT Services virtual private network (VPN) software. All other remote access technologies is prohibited, including access using bastion hosts, 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. Remote access to end user desktop equipment is prohibited.

Individuals wishing to implement alternative remote access technologies must obtain prior permission from IT Services.

If you remotely access University systems then you must ensure that the following security controls are in place:

- Remote access to University systems must use IT Services VPN or a previously approved remote access technology. Remote access to end user desktop equipment is prohibited.
- IT Services VPN must only be used for University related purposes. Use of IT Services VPN for personal use such as video streaming is prohibited.
- The device you are using for remote access must have sufficient protection in terms of malware protection, up to date o/s and application patches.
- You must have a strong UCD Connect password which conforms to IT Services password security standards.
- You must not attempt to log on to the VPN using another individual's credentials or a generic or group account.
- Caution should be exercised when accessing any University system or application on an untrusted network. Account holders should use the University VPN when accessing confidential systems or sensitive University information on untrusted networks e.g. Airport Wi-Fi, Conference Centre Wi-Fi, Hotel Wi-Fi, etc.

4. Related Standards, Policies and Procedures

- University Acceptable Use Policy
- University Data Protection Policy
- IT Services Password Protection Standards

Revision History

This guide is regularly reviewed and updated.

Date of Change	Responsible	Summary of Change
May 2017	IT Security	Version 1 (1.5)