Remote Access Security Policy

Controlled Document – refer to Intranet for latest version

Category: Information and Technology	Date Created: September 1997
Responsibility: Director Information Systems & Technology	Date Last Reviewed: September 2012
Approval: Chief Financial Officer	Version: 12.1

Purpose

It is essential to ensure that all access to the UCOL computer networks are controlled and the information systems contained within are protected from unauthorized access or interference.

It is frequently necessary to provide access to the internal network from off-campus. This Policy ensures that such access is provided over a secure circuit and reduces the possibility of unauthorised access to UCOL's Information Systems.

Scope

This Policy applies to **every person** who seeks to gain access to the **non-public** areas of the network.

Policy Statements

Access to the UCOL Network may be granted to staff, students and third parties contracted to carry out work on behalf of UCOL subject to the following conditions: -

- Under no circumstances is a Laptop, Workstation or Fileserver to be connected to the Public Switched Telephone Network whilst connected directly to the UCOL Internal Network unless specifically authorised by the Director of Information Systems and Technology or his authorised delegate.
- **All** remote access shall be conducted through a Virtual Private Network (VPN) unless otherwise approved by the Director of Information Systems and Technology or his authorised delegate.
- Access to the Web server and E-mail services are available via the Internet and do not require remote access facilities.
- Off-Campus access to the UCOL Internal Network will be granted for the period that a person has an account on the UCOL network.
- All requests for remote access to specific servers, (RDP) shall be in writing giving the reasons for requiring remote access. If RDP access is granted it will be limited to the period specified in the request and to the person making that request. The provisions of UCOL's Information Systems Security Policy relating to password protection and access rights shall apply to all users accessing the network through the VPN or RDP.

- Access rights to a third party shall be granted only on application from a designated Systems Manager who will be responsible for controlling that third parties access rights on the network. Access will be implemented in accordance with UCOL's Information Systems Security Policy. The Systems Manager will be responsible for logging all remote access made by the third party.

Definitions

Remote Access

Off-Campus access to the UCOL Internal Network.

VPN

Virtual Private Network requiring the user to connect to the UCOL network via the Internet over an encrypted secure path using a UCOL computer account.

RDP

Remote Desktop Protocol: a means by which users use a remote desktop to take control of a server or another desktop.

UCOL Internal Network

The interconnection of laptop, workstations, network servers and other peripheral devices established by UCOL and requiring access via a user account and password.

Information Systems

Specific applications and associated data used by UCOL to carry out its day-to-day activities.

CE

The Chief Executive of UCOL[tm] Universal College of Learning or his authorised delegate.

Systems Manager

The individual employee delegated responsibility for the management of a Section/Faculty information system or application by the Head of Section/Faculty.

Relevant Legislation

Employment Relations Act
Education and Training Act 2020

Related Documentation

- Academic Statute - Section 28, Discipline
- Disciplinary Procedure
- Computer Use Policy
- Information Systems Security Policy