Information Systems 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

Staff have a responsibility to protect the information systems and data to which they have access. This Policy seeks to ensure that access to electronic data stored on UCOL fileservers and local hard drives is available only to those users who are authorised to access that data.

The information stored on UCOL's computer networks represents a significant investment on the part of the individual and the organisation.

This policy establishes guidelines for employees, students and contractors who may be given access to the computing system. This policy promotes the responsible and secure use of computing resources at UCOL.

Scope

This Policy applies to **everyone** who uses the computer facilities owned, leased, operated or contracted by UCOL.

Policy Statements

A designated Systems Manager will manage each of UCOL's information systems and applications. Each designated Systems Manager will be responsible for ensuring that appropriate access controls are in place and that access is only made available to persons who have a need to access the systems in the course of their employment or study.

It is the responsibility of Heads of Section and Faculties to delegate responsibility for the management of each of the systems under their control to a Systems Manager and to advise the Director Information Systems and Technology of the name and location of persons so designated.

Access to UCOL's information systems and applications will be made available to users who:-

- have been individually authorised to access a system by the designated Systems Manager; or
- have been granted specific access rights by virtue of their employment or enrolment status; or
- have been granted access by the CE; or
- are accessing publicly available areas of the network.

Attempting to access systems for which no authorisation has been given will constitute a breach of this Policy and may be treated as serious misconduct.

Individual users have a responsibility to protect the information and systems under their jurisdiction. In particular users are required to:-

- keep their passwords confidential and change them not less often than once every 30 days;
- choose passwords which do not form words or patterns and which contain at least one non-alphabetic character;
- ensure that they make frequent copies of their work to the network drive;
- protect their work station from unauthorised access by means of a password protected screen saver and/or by closing down and logging off whenever they leave their work area unattended.
- ensure all e-mail attachments and floppy disk drives are scanned for viruses before opening any files contained therein;
- report any unresolved virus problems to the IT help desk;
- report any suspected breaches or attempted breaches of the computer security systems to the UCOL Director of Information Systems and Technology.

Definitions

Workstation

Computer equipment, i.e. CPU, keyboard, mouse, monitor.

Network

The interconnection of workstations, network servers and other peripheral devices

Information Systems

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

Applications

Computer programs available to users logged on to a workstation.

CE

The Chief Executive of UCOL or their authorised delegate.

Systems Manager

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

Relevant Legislation

- Employment Relations Act 2000
- Education and Training Act 2020

Related Documentation

- Academic Statute, Section 28, Discipline.
- Disciplinary Procedure
- Computer Use Policy