UNIVERSITY COLLEGE CORK

IT Security Policy

Document Location

http://www.ucc.ie/en/it-policies/

1. Introduction

The objective of this security policy is to promote a culture that helps maximise the value of information through its efficient management and secure protection as well as safeguarding the University and the rights of staff, students and other parties who depend on the information or to whom it relates. In particular the policy is aimed at:

- Safeguarding the availability, confidentiality and integrity of the University's information.
- Protecting the IT assets and services of the University against unauthorised access, intrusion, disruption or other damage.
- Ensuring compliance with relevant legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.

All staff and students must comply with this policy. Third party users undertaking work with or for the University must also comply with the policy. The policy would not generally apply to external users accessing the services of the University via the Web.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply could lead to the cancellation of a contract.

2. Scope

This policy applies to all IT services and systems provided centrally by the Computer Centre as well as those provided locally in offices, departments, schools, colleges or other units.

It applies to the UCC network and connected networks and to all equipment connected to those networks physically or via wireless.

Should any networks be created independently of the campus network, they will have to comply with this policy if they are connected to the Internet.

The policy applies to all UCC-owned IT equipment including servers, desktops, laptops, PDAs and other mobile devices, network-related equipment, as well as personally-owned equipment used by staff or students in conjunction with their work or study in UCC.

Note that access to and the use of UCC–related electronic information and data are covered by UCC data management policy.

3. Supporting Policies

The following subsidiary policies, procedures and standards shall be considered part of this IT Security Policy:

§ Acceptable Use Policy

§ Code of Practise

§ Communications Policy

§ Peer-to-Peer Policy

§ Personal Websites Policy

§ Policy for the 'All Exchange Users' Mailing List

§ Procedure Relating to Access to Staff Accounts

§ Procedure Relating to Access to Student and Alumni Accounts

§ Standards for Network Points

§ Structured Cabling System Standard

§ Standards for Connecting Equipment to the UCC Network

In addition, the following legislation must be considered in conjunction with this policy:

§ The Data Protection Act (1988/2003)

§ Child Trafficking and Pornography Act (1998)

§ Intellectual Property Miscellaneous Provisions Act (1998)

§ Copyright and Related Rights Act (2000)

§ Safety, Health and Welfare at Work Act (2005)

§ Criminal Damage Act (1991)

This policy has been approved by the Governing Body. Any additions or amendments to this or related policies will be submitted by the University Management Team Strategic (UMTS) to the Governing Body for approval or to whatever authority the Governing Body may delegate this role.

The policy will be reviewed, at least annually, by the Director of the Computer Centre who will consult as necessary before submitting any amendments for approval.

4. Policy Provisions

1) Every student and staff member in UCC is provided with access to the UCC network and various services on the network. They are required to familiarise themselves with the relevant policies, procedures and standards and to comply with these at all times. The up-to-date versions of the policies are available on the Computer Centre website and anyone requiring further information, clarification or advice should contact the Computer Centre Helpdesk in the first instance.

2) The Computer Centre is responsible for the development, management and maintenance of the UCC network and no equipment or sub-networks may be connected to the UCC network unless authorised by the Computer Centre.

3) Each piece of equipment connected to the network must have as an identifiable 'owner', a staff member who will be responsible for ensuring that the connected equipment complies with the relevant policies and regulations. In cases where someone other than a member of staff is connecting equipment, they must first have the written permission of the relevant head of department, school or college who will take responsibility for the connection and for informing the Computer Centre when that user no longer requires the connection. In the case of events such as conferences, the local UCC organiser will be responsible for connections made by any of the non-UCC attendees. Where a UCC staff member is taking responsibility for non-UCC users on the network, they are obliged to inform the users of their obligations under the Acceptable Use Policy.

4) The Computer Centre has the authority to remove from the network any equipment for which no owner can be identified.

5) The Computer Centre has the authority to remove from the network any equipment which is interfering with the network service or is deemed likely to compromise the security of the network. While every effort will be made to contact the owner of the equipment in advance, maintaining the service must take precedence.

6) Anyone connecting equipment to the network is responsible for ensuring that the equipment is configured correctly, that the operating systems and software applications are up-to-date as regards patch management etc. and that the equipment has adequate protection against viruses and other malware. If there is any suspicion that the equipment may be infected or compromised in any way it should not be connected.

7) Users of portable devices and media must take suitable precautions to protect information contained thereon against loss or damage, and to prevent infection by malware.

8) Any servers hosting production services for the University must be housed in a suitable environment with regard to security, electrical power, air cooling etc. The owner of the server must ensure that all software licenses are up-to-date and that maintenance support is available for both the hardware and software. Provision must be made for adequate backup and documented operating procedures must be available.

9) It is the responsibility of the business owner of each service to ensure that an adequate business continuity plan is in place in the event that the service is affected by the non-availability of the relevant servers, network or other elements of the IT infrastructure.

10) Authentication is required for each connection to the network. Authentication is normally via a password or PIN. It is the responsibility of each user to ensure that their password or PIN is not disclosed to anyone. In the rare event that a member of the Computer Centre staff requests a user's password from them to rectify a problem with their system, the user should change their password immediately afterwards. Users should never send their passwords or other identity information via email, fax, post etc.

11) Any breaches of security should be reported immediately to the Computer Centre Helpdesk.

This security policy is intended to ensure an effective IT infrastructure for the benefit of all users. Where necessary, support will be provided by the Computer Centre to assist users in complying with the policy

5. Further Information

If you have any queries in relation to this policy, please contact:

Director of the Computer Centre

University College Cork

Tel: 021 4902215

Email: it_director@ucc.ie

- *Approved by the UCC Governing Body – 19th April 2011*