In This Section

IT Security Policy

IT Security Policy

Print

Version Number: 1.2

Revision date: Tue, 19 Sep 2017 09:14:00 IST

Policy Owner: Director of IT Services

Policy Contents

1 Purpose

The purpose of this IT security policy is to protect the information assets of the University from all threats, internal, external, deliberate or accidental. The policy is aimed at:

SAVE TO FAVOURITES SHARE

- 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 applicable legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.

The policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

Back To Top

2 Policy Scope

This IT Security Policy covers documentation of policy, procedures and standards relating to:

- University College Cork Information Assets
- University College Cork IT Resources

This Policy applies to all Users of the University's IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices. This Policy takes precedence over any policies which may be developed at a local level.

Back To Top

3 Roles and Responsibilities

The roles and responsibilities for governance for IT Policy are outlined in the master .

IT Services is responsible for monitoring use of University IT Resources to ensure this Policy is not breached.

IT Security Officer is responsible for enforcing effective operation of the Information Security Policy to ensure that information assets and technologies are adequately protected.

All users, students and staff are required to demonstrate compliance to UCC'S Information Security Policy in order to protect the confidentiality, integrity, and availability of UCC's Information Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to UCC.

Back To Top

4 Policy Text

SAVE TO FAVOURITES SHARE

Confidentiality

- Data Management
- Network Security
- User Authentication
- Encryption
- IT Security Training

Integrity

- User Access
- Vulnerability Management
- Change Management

Availability

- Software Licensing
- Disaster Recovery
- Incident Management
- Security Operations
- Physical Security

4.1 Confidentiality

Safe guarding the confidentiality of information through the protection of information from unauthorised disclosure with access only by entitlement.

4.1.1 Data Classification and Management

- University College Cork is obligated to respect the rights of individuals and to protect confidential data.
- All university digital records should be classified according to the Data Classification Procedure.
  https://www.ucc.ie/en/media/support/itpolicies/procedures/DataClassification.pdf (https://www.ucc.ie/en/media/support/itpolicies/procedures/DataClassification.pdf)
- When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Please refer to University Data Governance Policy.
  https://www.ucc.ie/en/media/support/itpolicies/policies/DataManagementPolicy.pdf (https://www.ucc.ie/en/media/support/itpolicies/policies/DataManagementPolicy.pdf)
- All University College Cork information is to be treated as confidential if not otherwise indicated.
- Where UCC engages the use of Cloud or external hosting services, which will host UCC data, the proposed solutions must be evaluated by the External Hosted Data Committee per the following process https://www.ucc.ie/en/it/services/externaldatahosting/ (https://www.ucc.ie/en/it/services/externaldatahosting/)
- Where data and servers on the UCC network are accessed by 3rd parties (suppliers, contractors, consultants) for support and maintenance provided to UCC, Third Party Access form with the accompanying Data Protection agreements must be built into the service agreement with the 3rd

4.1.2 Network Security

SAVE TO FAVOURITES SHARE

- UCC maintains a perimeter firewall. All externally facing services must be registered, this register is used to configure the firewall based on the services they offer. This eliminates low

level vulnerability probing attacks from the internet while allowing access to registered services.

- In addition to the perimeter firewall, some network ranges are protected by access-lists or additional firewalls.
- Perimeter traffic is logged and appropriately monitored for security purposes.
- Laptops and Desktops that connect to UCC's internal network should have:
    - Anti-virus installed and up-to-date,
    - Operating System patched with latest security updates
    - Personal Firewall active
    - User authentication
- Please reference the following technical documents in relation to the connection of additional equipment to the UCC network.
https://www.ucc.ie/en/media/support/itpolicies/standards/ConnectingEquipmentUCCStanda
(https://www.ucc.ie/en/media/support/itpolicies/standards/ConnectingEquipmentUCCStanda

4.1.3 User Authentication and Audit Logging

- Authentication is required for each connection to the network.
- Where possible Two factor authentication should be considered for IT Systems that process sensitive data.
- All UCC IT systems must comply to UCC's password policy:
https://www.ucc.ie/en/it/services/pwpolicies/
(https://www.ucc.ie/en/it/services/pwpolicies/)
- User must follow best practices to prevent misuse, loss or unauthorised access to systems:
    - Keep passwords confidential
    - Change passwords regularly
    - Never write down passwords
    - Never send passwords via email, fax or post
    - Change temporary passwords at first logon
- Do not leave your computer unattended without locking your computer or logging off.
- Audit logs containing the following user events of staff, students and any 3rd parties accessing the UCC network are captured and monitored:
    - User IDs
    - Dates and times for logon and logoff
    - Computer identity and location where possible
    - Records of successful and rejected system access attempts
    - Records of successful and rejected system access attempts
    - Monitoring of privileged user accounts

SAVE TO FAVOURITES SHARE

4.1.4 Encryption

- All University owned laptops must have their internal hard drive encrypted. This is a service supported by IT Services per https://www.ucc.ie/en/it/services/encryptionlaptop/ (https://www.ucc.ie/en/it/services/encryptionlaptop/)
- All University provided mobile devices that host UCC data (email) must be protected by encryption and layered authentication where appropriate.
- Where personal data is being stored by UCC on a laptop or portable device, that may leave UCC premises, then this data should be encrypted in accordance with the UCC Encryption (http://www.ucc.ie/en/media/support/itpolicies/guidelines/EncryptionGuidelines.pdf)guidelin and ensure compliance with the UCC Data Protection policy
- Where sensitive information is transmitted through a public network to an external third party the information must be encrypted first and sent via secure channels (SFTP, SSH, HTTPS, VPN etc.)
- WIFI networks advertised for staff business use (EDUROAM) must be encrypted using WPA2 or better.

4.1.5 IT Security training

- IT Security awareness strategy is delivered through multiple methods with the aim of raising user awareness and highlighting end user responsibilities.
- Scheduled targeted Security Awareness Training sessions are available on demand in conjunction with Data Protection training.
- Comprehensive online training sessions are available via the IT Security module in the ECDL training free of charge for all staff.
- On staff induction new hires are briefed on the Data Protection Policy and the IT AUP policy.

4.2 Integrity

Safeguarding the integrity of information, i.e. the accuracy and completeness of information by protecting against unauthorised modification.

4.2.1 User Access and Audit Logging

- Access to information is granted on a needs only basis, staff are granted specific access to allow them to carry out their job functions. Please refer to https://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToITServices.pdf (https://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToITServices.pdf)
- Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.
- All individuals have a unique user ID (end users, DBA's, network admin, programmers) for their personal and sole use so that activities can be traced to the responsible person
- Access to code, OS, code, services and commands is restricted to only those individuals who require access as part of their day-to-day job responsibilities.
- All access to high criticality services is to be logged and appropriately monitored to identify potential misuse of systems or information. Logs must be retained and access granted according to the appropriate legislation.
- Security event logs, operational audit logs, error logs, transaction and processing logs are monitored on critical systems and retained to record events for trouble shooting, provide

SAVE TO FAVOURITES SHARE

forensics during security incidents and to identify potential misuse of systems or information.

- An appropriate audit trail including database logs of the creation, amendment and deletion of UCC data and/or systems is maintained by IT Services. This is particularly important in relation to the following:

    - Data including details on staff, students and suppliers;
    - Data including inward fee payments, outward supplier payments, and payroll transactions;
    - University College Cork – National University of Ireland resource usage data.
    - University College Cork – National University of Ireland data which may reside outside main University College Cork – National University of Ireland system(s). This could include data which resides on external cloud services or data that resides on internal such as Excel Spreadsheets, local desktop databases etc.

4.2.2 Vulnerability Management

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 it should not be connected.

- Each IT Service has a defined service owner. Server's supporting this service must be hardened appropriately before joining the UCC network and should be locked down before becoming a production service. This is the IT Service owner's responsibility.
- UCC infrastructure (servers, desktops, operating systems, databases and applications) must follow a regular patch schedule to ensure IT Assets remain protected from security vulnerabilities and remain within mainstream support.
- Antivirus is compulsory pre-requisite for any computer joining the UCC network. Anti-virus is controlled centrally from IT Services https://www.ucc.ie/en/it/services/antivirus/ (https://www.ucc.ie/en/it/services/antivirus/)
- The University's IT Services has the authority to remove from the network any equipment for which no owner can be identified.
- The University's IT Services 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, maintining the service must take precedence.

4.2.3 Change Management

System changes should be completed in accordance with the IT Services formal change management process with audit trails for changes to highly critical systems.

4.3 Availability

Maintaining the availability of the University's information and IT systems for business processes usage as required.

SAVE TO FAVOURITES SHARE

4.3.1 Software Licensing and Maintenance

- Each IT Service has a defined service owner. The service owner must ensure that all software licenses are up-to-date and that maintenance support is available for both the hardware and software associated with their service.
- Desktop software licencing for standard software is managed centrally through site licensing for staff. Licensing for non-standard software is the users responsibility: https://www.ucc.ie/en/it/services/software/ (https://www.ucc.ie/en/it/services/software/)
- Illegal and unlicensed software must not be installed on UCC owned computers

4.3.2 Disaster Recovery and Backup Strategy

- 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. Prevention of data loss through data back-ups.
- IT Services maintain Disaster Recovery plans for all UCC centrally managed infrastructure and critical services.
- Disaster Recovery plans and processes are tested regularly
- IT Services manage Data and system backups for critical systems
- Recovery from backup is tested regularly

4.3.3 Incident Management

Formal incident management procedures are in place for IT Security incidents and procedures relating to personal data breaches. Please reference IT Policy (https://www.ucc.ie/en/it-policies-2017/policies/it-policy/#breach) for policy breach process

4.3.4 Security Operations

UCC IT Services manage multiple security tools with the aim of protecting the IT assets and services of the University against unauthorised access, intrusion and disruption. Processes are in place to support these tools and ensure proactive management of IT vulnerabilities and reported incidents.

4.3.5 Physical computer storage Environmental provisions

Any servers hosting production services for the University must be housed in a suitable environment with regard to security, electrical power, air cooling etc.

- All hardware used for the storage of University College Cork – National University of Ireland data is to be purged of data and securely destroyed once it is no longer to be used. See our guidelines on the disposal of devices containing confidential data (http://www.ucc.ie/en/media/support/itpolicies/guidelines/DisposalOfDevicesGuidelines.pdf)
- When tapes and other secondary storage devices reach the end of their useful life they are to be purged of UCC Data and securely destroyed.

SAVE TO FAVOURITES SHARE

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 IT Services to assist users in complying with the policy.

4.4 IT Security Governance

IT Security is governed in UCC through

- Internal Audit (https://www.ucc.ie/en/internalaudit/internalauditsystemofinternalcontrol/ (https://www.ucc.ie/en/internalaudit/internalauditsystemofinternalcontrol/))
- Yearly External Audit for financial systems
- UCC Risk Register (https://www.ucc.ie/en/ocla/risk/ (https://www.ucc.ie/en/ocla/risk/))

Back To Top

5 Supporting Procedures, Policies and or Statutes

The Policy should be read in conjunction with the following UCC policies and users should ensure compliance with these policies in addition to this policy. The following subsidiary policies, procedures and standards shall be considered part of this IT Security Policy:

- IT Policy Framework (/en/it-policies/policies/it-policy/)
- Acceptable Usage Policy (/en/it-policies/policies/au-pol/)
- Web and Social Media Policy (/en/it-policies/policies/sm-policy/)
- Access to IT Services Procedure (https://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToITServices.pdf)
- Data Management Policy (http://www.ucc.ie/en/media/support/itpolicies/policies/DataManagementPolicy.pdf)
- Data Classification Policy (https://www.ucc.ie/en/media/support/itpolicies/procedures/DataClassification.pdf)
- UCC Data Privacy Policy (http://www.ucc.ie/en/it-policies/policies/privacy/)
- Procedure Relating to Access to Staff Accounts (http://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToStudentAccounts.pdf)
- Procedure Relating to Access to Student and Alumni Accounts (http://www.ucc.ie/en/media/support/itpolicies/procedures/AccessToStudentAccounts.pdf)

Back To Top

6 Breach of Policy

As per the IT Policy Framework (https://www.ucc.ie/en/it-policies/policies/it-policy/#breach)

Back To Top

SAVE TO FAVOURITES SHARE

7 Review and Approval

The University reserves the right to amend this Policy at any time in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.

Any such revisions will be noted in the revision history of the policy, which are available to you on the website and by continuing to use the University's IT Resources following any updated you will be deemed to have accepted the revised terms of this Policy.

Summary of Policy Changes

Revision History

Date of this revision: 19/09/17	**Date of next review: 19/09/18**

Version Number/Revision Number	**Revision Date**	**Summary of Changes**
0.1	19/04/2011	Approved by Governing body
O.2	26/05/2014	Updated to reflect new name of IT department and include encryption requirement
1.1	30/09/16	2016 Review: updated broken links. Removed old comments.
1.2	19/09/2017	Re-structuring of content and creation of sections under Confidentiality, Integrity and Availability Inclusion of Firewall

Consultation History

Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**

SAVE TO FAVOURITES SHARE

Approval

This document requires the following approvals:

Name	Title	Date
Gerard Culley	Director of Information Technology	
John Fitzgerald	Director of Information Services	
John Morrison	Chair of IS & AR committee	
Michael Farrell	Corporate Secretary	

This policy shall be reviewed and updated on an annual basis.

8 Further Information

Contact Email:itsecurity@ucc.ie

Contact Name:

Director of IT Services
Contact Telephone Number:

021 4902215

Back To Top

SAVE TO FAVOURITES

SHARE

Definitions

This Policy provides clear guidance on the responsibilities of Users of the University's IT Resources and Network Services.

For the purposes of this Policy, the following capitalised terms (which are used throughout this Policy) shall have the following meanings in the context of this Policy:

Term	Definition
Information Security	The process of implementing measures and systems designed to secure protect and safeguard information utilising various forms of technology developed to create, store, use and exchange such information against a unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrit availability, intended use and its ability to perform their permitted critical functions.
Digital Estate Working Group (DEWG, dewg@ucc.ie (mailto:dewg@ucc.ie))	The DEWG manage the day-to-day running of the University's websites ar social media presence. It is comprised of: ■ IT; ■ Marketing and Communications; ■ Media and Public Relations; ■ Registrar's Office. For more information reference the Digital Estate Governance Policy Digi Estate Governance Policy (https://www.ucc.ie/en/media/support/itpolicies/policies/DigitalEstatev
External Hosting Group	The External Hosting Group chaired by the University IT Security Officer i responsible for approving the hosting of corporate data and information premise and in third party data centres. Included in this group is the Data Protection Officer and the Legal Secretary who will advise data owners o matters of data protection and legal matters. This group is also tasked w advising and directing a response to any IT Policy breach relating to corp data or resources.
External Parties	All the University's subsidiary companies, contractors, researchers, visito and/or any other parties who have access to the University's IT Resource
Policy	This AUP Policy.
Staff	All full-time and part-time employees of the University, including researcl funded externally

SAVE TO FAVOURITES SHARE

Student	A Student, either full-time or part-time, registered with UCC.
University Information Assets	Information which is of value to the University. This includes, but is not li to, information regarding: ■ Students; ■ Staff; ■ financial matters; ■ This information may be stored on many different media including: ■ paper; ■ electronic hardware devices (hard drives, flash drives); ■ centrally managed infrastructure including servers and storage; ■ mobile devices; ■ cloud hosted services.
University IT Resources	IT resources include those provided centrally by the University's IT Servic well as those provided locally in its offices, departments, schools, colleg other units. This includes University IT resources accessed remotely via without limitation: ■ The University's network and connected networks and to all equipn connected to those networks physically or via wireless. ■ Any networks created independently off the campus network, if the connected to the University network. ■ All University-owned IT equipment including servers, desktops, lapt tablets, mobile devices and network-related equipment. ■ Any equipment owned by third parties, leased or personally-owned use the University network, in conjunction with their work or study i University.
University or UCC	University College Cork – National University of Ireland, Cork
Users	All Students, Staff and External Parties.

Back To Top

SAVE TO FAVOURITES

SHARE

Procedures

(/en/it-policies/procedures/)

Guidelines/Standards

(/en/it-policies/guidelines/)

SAVE TO FAVOURITES

SHARE

Standards

(/en/it-policies/standards/)

University College Cork

Coláiste na hOllscoile Corcaigh

College Road, Cork T12 K8AF

+353 (0)21 490 3000 (tel:+353 (0)21 490 3000)

Lo
(https://www.google.ie/maps/place/University+College+Cork/@51.8889472,-8.474624,14
8.493

University College Cork

Bring me to

SAVE TO MyUCC FAVOURITES

SHARE

Show me

Copyright © UCC 2017

SAVE TO FAVOURITES

SHARE