National University of Ireland Galway

ICT Security Policy 2005

NUI, Galway ICT Security Policy

Introduction

Modern Information and Communications Technology (ICT) is increasingly capable of supporting “work anywhere” and “work with anyone” models for teaching and research and for administrative activities. The University therefore recognises the need to support the activities of its staff and students both on-campus and at other locations worldwide, from which they may require to securely store, transmit, access or exchange information connected with the University’s activities.

The University recognises that modern ICT security is an issue for the whole University community. Modern technology can enable the rapid proliferation of attacks and exploits, which undermine the success of the University. The actions of one member of the community can produce an adverse effect on the whole community. Furthermore, the University can be adversely affected by actions that take place far away from campus.

The University has therefore decided to introduce the policy set out below for managing the risks associated with ICT.

The policy is designed to be generic, recognising that the specific technologies in use and the associated risks will change over time.

Definitions

Campus
The University’s main campus is situated in Galway City. Other facilities are located in An Cheathrú Rua, Carna, Mace Head, Carron and Gaoth Dobhair.

Heads of Units
The person responsible for the management of an organisational unit within the University.
(An organisational unit may be an academic department, research unit, administration service or other unit with the University.)

ICT Assets
All information systems used to store or transmit any information stored by or on behalf of the University or any User included within the scope of this policy, for any purpose including teaching, research and administration. These information systems include but are not limited to all infrastructure, networks, hardware, software, and data storage devices.

Networks
All physical and technical infrastructure and devices and services utilised to provide the University’s network and network services.

Owners
The owner of an ICT Asset is the person with overall business or academic responsibility for the ICT Asset, irrespective of actual legal ownership.

Security
Security is the preservation of:

- Confidentiality: ensuring data is available to authorised persons only;
- Integrity: ensuring data is accurate and complete;
- Availability: ensuring that authorised users have access to data and ICT Assets when required.

Service Providers
Service providers are persons who use ICT assets to provide services to University Users, whether they are located on the University campus or otherwise.

Students
Students include currently registered students (including visiting students), as well as prospective, and former students of the University.

University Staff
University staff includes permanent and temporary academic staff, academic visitors (including research students) and permanent and temporary administrative staff (including persons on any type of placement or work experience assignment).

Users
Users of ICT include but are not limited to:

- All Students and University Staff;
- Other persons and organisations working with or on behalf of the University;
- Any other person who has been explicitly registered as a user of any of the University's ICT Assets or computer networks, or who has otherwise been explicitly authorised to use such resources;
- Any other person accessing or attempting to access any University ICT Asset to which public access has been provided;
- Any other persons using the University's ICT Assets to do business with the University, whether as a researcher, contractor, consultant or supplier.

Scope

This policy along with supporting guidelines and codes of practice, applies to all of the University's electronically stored data and ICT Assets and all Users both on-campus and at other locations worldwide.

This policy along with supporting guidelines and codes of practice is mandatory for all Users.

Exclusions

- Manual Information Systems;
- Self-contained systems which have no capability to connect to any University network and which have no capability to store information for or on behalf of the University or any User.

Policy

Policy Statement
Under this policy the University, through the Governing Authority, the Computing Strategic Planning Committee, responsible managers, and Heads of Units, shall:

- Assign an owner to all ICT Assets.

- Ensure that an approved risk assessment process is used to identify those risks to which each ICT Asset may be exposed.

- Take the appropriate steps to manage the technological risks associated with storing, transmitting, accessing and exchanging information in support of its academic and administrative activities.

- Ensure that ICT Assets are adequately protected against loss, misuse, or abuse.
- Ensure that information is created and maintained in an environment whose level of security matches the academic and administrative value of the information.

- Approve this policy and all supporting policies.

- Create awareness of this policy and supporting policies to all Users by publishing them to the University's website and elsewhere as appropriate.

- Ensure that activities conducted by the University abide by all relevant Irish and European Community legislation.

Key Roles and Responsibilities

Údarás na h-Ollscoile
Údarás na h-Ollscoile is responsible for approving this policy.

Asset Owners
Owners are responsible for:

- Securing the ICT Assets owned by them;
- Completing and documenting a formal risk assessment of their ICT Assets and taking prompt and proportionate actions in response to the findings;
- Controlling access to each of their ICT assets to a level of security that matches the academic and administrative value of those assets;
- Reporting suspected or actual breaches to the security of ICT Assets.

Computing Strategic Planning Committee (CSPC)
The CSPC or its successor bodies are responsible for discussing and agreeing any changes to this policy and all supporting policies, standards and guidelines. This work is subject to the oversight of Údarás na h-Ollscoile.

Director of Computer Services
The Director of Computer Services is responsible for:

- Ensuring that appropriate advisory, monitoring, reporting, and review processes are in place to enforce this policy;
- Supporting Asset Owners in achieving compliance with the policy;
- Publishing this policy and supporting guidelines and codes of practice to the University's website and elsewhere as appropriate;
- Working with other University offices to ensure that this policy is integrated with student disciplinary codes and with the University's contracts of employment;
- Reporting to the CSPC at least annually on the operation of this policy.

Internal Auditor
The Internal Auditor is responsible for monitoring compliance with this policy.

Heads of Units
Heads of Units are responsible for

- identifying all business and academic ICT Assets within their area of responsibility,
- assigning owners to each ICT Asset, and,
- working with Asset Owners in their area of responsibility to assist them achieve compliance with the policy.

Working with the Director of Computer Services, Heads of Units are responsible for ensuring that appropriate risk management, security countermeasures and operational processes are in place to ensure that systems and networks owned within their unit are compliant with this policy and with codes of practice which have been put in place.

Service Providers
Service Providers are responsible for applying this policy to the ICT assets for which they have responsibility and for providing advice to users.

Users
Users must familiarise themselves and comply with this policy and all supporting policies, standards and guidelines.

Monitoring and Enforcement

Monitoring

- Working with the Director of Computer Services, Heads of Units and Asset Owners will monitor, report, review, and audit ICT Assets across the University to ensure compliance with this policy.

Any person suspecting that there has been, or is likely to be, a breach to the security of ICT Assets should immediately inform the Director of Computer Services or a nominated person acting on his/her behalf.

Enforcement
The Director of Computer Services or nominated persons acting on his/her behalf has the authority to enforce this policy. Enforcement may ultimately involve taking immediate measures or counter measures to protect the collective interest of the University community.

Disciplinary Procedures
Failure to comply with this policy and all supporting policies, standards and guidelines may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action.

Revision

This policy may be changed by decision of Údarás na h-Ollscoile. Any proposed change shall first be discussed and agreed by the University's CSPC.

This policy will take effect once it has been approved by Údarás na h-Ollscoile and shall apply until further notice.

Updates to this policy will be made periodically and will be published to the University's website and elsewhere as appropriate.

Guidance

This policy, along with supporting guidelines and codes of practice, is published on the University's website and elsewhere as appropriate.