NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: **QA411**
Title: **End User Policy**
Date: July 2018
Approval: ICT Security Committee

1. Purpose

To ensure continuity of our University and to minimise damage from incidents, it is essential that we embed a minimum set of security standards to protect the University. This policy is developed to protect NUI Galway from all threats, whether internal or external, deliberate or accidental.

In support of its mission of teaching and research, NUI Galway provides access to computing resources for students and staff of the University. Access to the University's computing facilities is a privilege granted to members of the University which can be withdrawn. The University reserves the right to limit, restrict or extend computing privileges and access to its information resources.

The policy is designed to ensure resources are utilised in an effective, efficient, ethical and lawful manner.

2. Description

This policy applies to:

- All Staff, and Students who have access to University IT Systems
- All contractors, vendors or others (including 3rd parties), who have access to University IT Systems.

It is the responsibility of each individual to read this and related security policies and be familiar with its contents. It is the responsibility of Academic Heads, and managers to ensure all staff using the IT systems are aware of and understand their responsibilities in this policy.

This document details information security rules and responsibilities for all users of NUI Galway IT systems and as end-user of these systems. Additional requirements specific to Asset Owners and administrators are not detailed in this policy.

3. Definitions

IT Resources. Software hardware (including networks) provided by NUI Galway to staff/students.

User/End User: Staff/Student contractor/visitor provided with access to NUI Galway IT resources.

"**Must**", or the terms "**required**" or "**shall**", refer to an absolute requirement of the policy.

"**Must not**" or "**shall not**", refer to statements which are an absolute prohibition of the policy.

"**Should**" or "**recommended**" refer to a statement that should be applied. In certain circumstances, there may be a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.

"**Should not**" or "**not recommended**" mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

University IT resources are the property of NUI Galway and are to be used for legitimate purposes only. This policy outlines the acceptable and unacceptable use of these resources

Acceptable use

1. Subject to clauses 4 to 11 below, NUI Galway IT resources may only be used as part of your duties as a member of NUI Galway or for educational purposes related to your activities at NUI Galway.
2. Users of IT resources must abide by all the licensing agreements for software entered into by the University with other parties, and not infringe any copyright of documentation or software.
3. Users are responsible for all actions undertaken using your user login/account, and will be held accountable for any misuse. Users must adhere to the university password policy and account passwords should never be shared with other users. User must never request login details or passwords from other users but must only use the credentials which has been issued to them by the University.

Unacceptable use

4. Users must not seek to gain unauthorised access to either the University IT resources or any other organisation and must not allow unauthorised access to the University's systems.
5. Users must not use another person's password or user account, even if they have left the University.
6. University IT resources cannot be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities.
7. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material (See Note 1).
8. Creation or transmission of material with the intent to cause annoyance inconvenience or needless anxiety.
9. Creation or transmission of material with the intent to defraud.
10. Creation or transmission of defamatory material.
11. Creation or transmission of material such that this infringes the copyright of another person.
12. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the University has chosen to subscribe.
13. Deliberate unauthorised access to networked facilities or services.
14. Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
    - 11.1 wasting staff effort or University resources and the effort of external suppliers involved in the support of those systems; corrupting or destroying other users' data;
    - 11.2 violating the privacy of other users;
    - 11.3 disrupting the work of other users;
    - 11.4 denying service to other users (for example, by overloading of access links or University network equipment) .
    - 11.5 continuing to use an item of software or hardware after the ISS department or its authorised representative has requested that use cease because it is causing disruption to the correct functioning of the University
    - 11.6 other misuse, such as the introduction of "viruses" or other harmful software via University IT resources.

11.7 Where IT resources are being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network is regarded as unacceptable use of NUI Galway IT resources.

11.8 Deactivation or disengagement of any protection mechanisms installed on IT resources (personal firewalls, antivirus software, administration account, etc.).

11.9 Users must not take advantage of a security incident or weakness in any system and must not facilitate others to do so.

Note 1: The list of unacceptable activities in this section is not exhaustive. The purpose is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse and potentially unlawful use of IT resources.

Note 2 It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use, and the responsibility for any such approval rests with the University and should be in line with the Universities guidance on handling sensitive research materials.

Compliance/Monitoring

If a user observe a security incident or weakness, they should report it as soon as possible. Attempts should be made to avoid taking actions which may contaminate any evidence or audit trail associated with activity. Incidents should be reported as quickly as possible to NUI Galway Information Solutions and Services (ISS) Service Desk, and to your Head of School or Unit.

1. If users suspect that unauthorised access to personal data has taken place then you must report the incident in accordance with the NUI Galway Data Protection Policy.
   In order to protect NUI Galway resources from internal and external threats whether deliberate or accidental, and to ensure compliance with regulatory and/or legal requirements, use of all IT resources and information passing through or stored on IT resources is subject to monitoring.
2. Users should be aware that there are tools in place to monitor the content of all incoming and outgoing emails and online activity and have no expectation of privacy while using the IT resources of NUI Galway.
3. Users must ensure appropriate anti-virus protection is active on all devices connecting to the university IT resources in line with the anti-virus and malware protection policy
4. It is your responsibility to read and be familiar with the contents of this policy. If you violate any of these policies, you may be denied access to University Information and IT Systems and may also be subject to other disciplinary action.

5. Responsibilities

Name	**Responsibility**
ICT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
ICT Security Committee	Approval of the Policy
All End-users (refer to end-user policies)	Responsible for implementation of the policy.
Internal and external audit	Monitoring and reporting compliance with the policy
ISS Service Desk	Tracking of calls related to Security Incidents

6. Related Documents /Attachments

QA400 Data Protection Policy
QA401 Data Handling
QA402 Data Classification
QA404 Password Policy
QA406 Remote Access Policy
QA408 Logical Access Policy
QA409 Encryption Policy
QA410 Anti-virus and Malware Protection Policy