NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA405

Title: Partnering Policy

Review Date: September 2020

Approval: University Management Team (UMT)

1. Purpose

It is envisaged that NUI Galway will partner with selected parties to provide ICT services. As security levels vary from one organisation to another it is important to ensure that a minimum level of protection is defined to protect NUI Galway.

NUI Galway requires that all partners meet an effective level of information security that is aligned with existing security policies (e.g. remote access, data handling and incident response policies). All partners must be made aware of their responsibilities and ensure that adequate protection is in place relative to the service being provided. Special security issues that relate to partnering include the following:

- The use of NUI Galway personal data;
- Access to NUI Galway systems;
- Any NUI Galway classified data stored on partner systems that may be compromised should it be stolen or lost.

The purpose of this policy is to ensure that effective measures are in place to limit any exposure to NUI Galway.

2. Description

This policy applies to all NUI Galway partners who provide ICT services for example, hosting a service, developing an application or to provide technical support services. This policy is not depended on the service being delivered on campus and is applicable in all cases.

It is the responsibility of the IT Asset owner to ensure the policy is implemented with all partners who process their data.

3. Definitions

"Partner" is defined as any organization providing a service to NUI Galway. This service may be on or off campus.

A **"Data Owner"** (sometimes referred to as a **"Business Owner", "System Owner",** or **"Asset Owner"**), is the person with overall responsibility for the system or service and in particular the data held. This should be the Manager or Head of function that commissioned the system or service and/or that owns the processes and data supported by the system or service. The Data Owner must be a NUIG staff, not a contractor or employee of a 3rd Party.

"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. Security Requirements

The following security controls apply:

1. The partner should have their own defined security policies, which should be supported by documented procedures, and in line with the NUI Galway Security Policies.

2. All partners or exchange of information must be compliant with all NUI Galway’s policies including, but not limited to, the Data Classifications and Data handling Policies, remote access policy, encryption policy, logical access policy.

3. A signed agreement/contract must be in place between NUI Galway and all partners.

4. The following criteria must be included in all agreements:

- a statement of compliance with the NUI Galway security policies.
- the contract must include a suitable Non-Disclosure Agreement (NDA), if applicable e.g. personal information is exchanged or NUI Galway intellectual property is divulged. ISS have a standard NDA which can be obtained from the Director of ISS on request.
- security responsibilities must be clearly defined including the security controls applied to NUI Galway data. This is also a legal requirement where personal data may be processed.
- a notification procedure and security incident management process
- right to audit and monitor compliance with the security requirements and controls of the agreement
- return or destruction of the information on completion of the agreement
- change management procedure
- service level and acceptable parameter indicators
- A statement of GDPR compliance

5. All contractual agreements with partners must have a specific contract clause stating that NUI Galway has the right to audit any service delivered on their behalf with prior notification. Compliance with the security requirements should be monitored.

6. When the development of a system is being performed by a partner, the following points must also be in the written contract:

- the ownership, intellectual property rights and licensing agreements of the developed software must be clearly defined.
- application security requirements must be clearly defined.
- the quality and security of the delivered software should be guaranteed by contract, making the third party responsible for any damages incurred by the company due to shortcomings in the software.

Before entering into a partnership with an external entity, NUI Galway must exercise due diligence in assessing the strategic, financial, operational, legal and reputational risks associated with the proposed partnership.

There is a partner management and review process in place for the continuous monitoring and evaluation of service delivery and compliance. Termination of a partnership arrangement must be carried out in a manner that ensures that NUI Galway's interests are protected.

5.0 Responsibilities

Name	**Responsibility**
ÌCT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
University Management Team	Approval of the Policy
Data Owners	Ensuring implementation of policy.
Internal and external audit	Monitoring and reporting compliance with the policy

6.0 Related Documents /Attachments

QA400 Data Protection Policy

QA401 Data Handling Policy

QA402 Data Classification Policy

QA404 Password Policy

QA406 Remote Access Policy

QA407 IT-Asset Protection Policy

QA408 Logical Access Policy

QA409 Encryption Policy

QA410 Anti-Virus and Malware Protection Policy

QA411 End User Policy