NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA399
Title: Cloud Services Policy
Review Date: September 2020
Approval: ICT Security Committee

# Purpose

To ensure continuity of our University and to minimise potential for incidents, it is essential that a minimum set of security standards exists to protect the University. This policy is designed to aid in the protection NUI Galway from risks & 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 Access to the University's IT facilities is a privilege granted to members of the University which can be withdrawn. The University reserves the right to limit, restrict or extend IT privileges and access to its information resources.

The policy is specifically designed to ensure resources are utilised in an effective, efficient, ethical and lawful manner when NUI Galway utilises any Cloud Services to aid in its business.

# Description

This policy applies to:
- All staff members responsible for provisioning or procuring Services which are Cloud based
- All owners of Cloud provisioned Services
- All third parties (including External Account holders) acting on behalf of the University provisioning procuring or amending Cloud Services

It is the responsibility of those staff types outlined above to read this and related security policies and be familiar with their contents.

It is the responsibility of all staff involved in the procurement of IT Services through Cloud, or hosted, capability to understand their responsibilities in relation to this policy (and related policies) and to ensure that all activities are in line with this policy.

# Definitions

This document provides information security rules and responsibilities for all users of NUI Galway IT systems and as end-user of these systems.

“**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.

**"End-User"** or **"Member of Staff"** or **"Staff Member"** refers to any employee whether temporary or permanent, NUI employed, or Agency employed or an External account holder within any area in NUI Galway.

**Cloud Service**; A cloud service is any service made available to users, on demand, via the Internet from a cloud computing providers server as opposed to these servers being provided from NUI Galway's premises.

**Cloud Service Types**; for the purposes of this policy Cloud Services are defined in four different delivery models;

**SaaS** - Software as a Service, where the Service Provider manages the entire solution

**PaaS -** Platform as a Service, where the cloud provider manages large elements of the solution

**IaaS** – Infrastructure as a Service, where the cloud provider manages only the infrastructure

**Bespoke Defined** – Where a specific method of provisioning the service has been agreed in advance by both parties, i.e. the user stakeholder and the cloud provider.

**Cloud services** *deployment* models:

• **Private cloud** – where services are provided by an internal provider, i.e. IS Services;

• **Public cloud** – where services are provided by third parties, i.e. external companies or entities, over the public Internet;

• **Hybrid cloud** – where services are provided partly by an internal provider in a private cloud and partly provided by an external company(s) or entity(s) in the public cloud.

**Cloud Service Owner;** The NUI Galway staff member/unit responsible, and accountable, for the sourcing of the service to the University.

# Requirements

1. A designated Cloud Service Owner must be declared, in writing, to the Data Protection Officer and Information Solutions & Services for all Cloud Services.

2. All University IT resources are the property of NUI Galway and are to be used for legitimate purposes only. As a procurer or provider of these services, it is the Cloud Service Owners responsibility to ensure that the University Assets are procured, evaluated and the ongoing use is in line with all relevant (Irish and European) legislation and university polices in place at the time – see related documents below.
3. The Cloud Service Owner must ensure the cloud service:
    a. Is fit for the purposes they have been obtained
    b. Is compliant with all relevant University Policies (including IT Security and Data Protection related policies).
    c. Is compliant with Irish and European legal and regulatory requirements
    d. Is procurement compliant as dictated by NUI Galway Procurement and Contracts Office.
    e. Is conformant with current Irish Public Service Guidance, i.e. a preference for all data residing within the Republic of Ireland or at a minimum within the EU (this includes, but is not limited to, backed up data)

f. That contractual clauses ensure NUI Galway data is returned to NUI Galway in the event of contract termination for any reason.
g. That the service is regularly audited under the guidance of NUI Galway internal audit to ensure that the service is compliant with NUI Galway's Policies.

4. All Cloud Service Owners shall be responsible for management of the following aspects of the service IT Security, Service, Incident, Problem, Release, Change, Configuration, Service Level Monitoring, Availability & Capacity, Service Continuity, and Financial.
5. All data held in within a cloud service on behalf of the University is considered University data and as such is subject to all relevant University policies, particular attention should be given to Data Protection Policy, the Data Classification policy Data Retention policy and all IT Security Policies. In keeping with these policies any sensitive data (Restricted or higher) should be encrypted at rest by the cloud provider.
6. Cloud Service Deployment Models shall adhere to the following model with data classification

| Data/Information Classification | Cloud Service Deployment Model | | | |
|---|---|---|---|---|
| | Internally Hosted/ Private Cloud or Hybrid with **appropriate** Security | NUIG Approved Public Cloud with Formal Security (ISO 27001, SOC 2 etc.) | Public Cloud without formal security | Other Model |
| Highly Confidential | Yes | Yes | No | Data Owner Approval |
| Restricted | Yes | Yes | No | Data Owner Approval |
| University Internal | Yes | Yes | No | Data Owner Approval |
| Public | Yes | Yes | Yes | Data Owner Approval |

7. ISS must be contacted at evaluation stage for advice where data from a cloud service is required to integrate with an internal University system. Provision of this data will be linked to compliance with this policy.
8. Access control is only permitted by federated Authentication through the University approved federation services.
9. Backup / Retention / Business Continuity / Disaster Recovery: The service must be selected to ensure that the data and information is secure at all times and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieved in a timely manner to meet business needs. For more critical systems, the service must be built with high availability, with a business continuity and disaster recovery plan that fits business needs. ISS must be contacted for advice and sign off in advance where a cloud services is being considered to provide a business-critical IT system
10. All third-party contract implication must be understood and addressed prior contracting with the cloud vendor
11. Formal approval must be gained from the Data Protection Officer, Director of ISS and the relevant

data/information owner (or their appointed nominees) prior to any new Cloud service being purchased or used for the first time for University business.

**Deviation from this policy will require ICT Security Committee approval**

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 who use or have access to NUI Galway IT system | Responsible for implementation of the policy. |
| Internal and external audit | Monitoring and reporting compliance with the policy |

# Related Documents /Attachments

QA400 Data Protection Policy
QA401 Data Handling
QA402 Data Classification
QA406 Remote Access Policy
QA408 Logical Access Policy
QA411 End User Policy
QA442 Record Retention Policy