NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA407
Title: **IT-Asset Protection Policy**
Date: July 2018
Approval: University Management Team (UMT)

1. Purpose

The purpose of the IT-Asset Protection Policy is to establish principles to effectively ensure significant IT-Assets are appropriately managed and controlled.

2. Description

The policy applies to:

- All staff and students who have access to University IT systems
- All contractors, vendors or others (3rd parties), who have access to University IT systems.
- All systems and production stages of development including production, test and development.

With particular emphasis on the roles and responsibilities of the Data Owner.

3. Definitions

An "**IT-Asset**" is defined as any system, device, or data owned or controlled by NUI Galway or that is utilised or accessed by NUI Galway staff/contractors, students or partners.

A "**Significant Asset**" is any tangible or intangible thing that has value to the university and therefore must be protected. This may refer to a specific system, service or data. Consumables such as PCs, Laptops, Mobiles while they are an IT-Asset would not be considered a Significant Asset.

An "**Asset Owner**" (sometimes referred to as a "Business Owner", or "System Owner"), is defined as the person with overall responsibility and accountability for the asset. The asset owner has responsibility for the assets maintenance, use and security as appropriate. The Asset Owner must be a member of NUI Galway staff, not a contractor or employee of a 3rd Party.

A "**Data Owner**" (sometimes referred to as the "Information Owner"), is defined by the University's Data Handling Policy as the "Individual or group responsible for classifying data and generating guidelines for its lifecycle management. These are usually the officers responsible for the initial collection/input and use of the data. The Data Owner must be a member of NUI Galway 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

1. All significant assets must be captured on an appropriate Asset Register.

2. All significant assets must have a designated **Data and/or Asset Owner**. This must be a NUIG employee, not a contractor or employee of a 3rd Party.

3. The **Asset and/or Data Owner** must define the security requirements, ensuring the continued operation, confidentiality and integrity of the significant asset and ensuring all security risks are appropriately managed on the systems, service or information for which they are responsible.

4. The Asset **Owner** must ensure the significant assets they are responsible for have an appropriate continuity strategy, business continuity and resumption plan(s).

5. The Asset and/or **Data Owner** must ensure appropriate security risk assessments are undertaken to check that the Significant Assets are sufficiently protected and are in line with security policy. To design cost effective security measures, a risk assessment is recommended to be carried out on Significant Assets, to establish the likely threats to the asset(s) and consequences of interference, damage or loss to the assets.

6. The Asset and **Data Owners** must ensure all Significant Assets for which they are responsible are compliant with NUI Galway security policies including, for example, Data Classification and Handling Policies, Password Policy, Logical Access Policy, Anti-virus and malware protection policy, partnering policy.

7. The Asset and **Data Owners** must ensure security compliance checks of systems are completed to validate compliance with the policy. System checks should include:
   - ✓ Anti-Virus is functional and updating (as per anti-virus policy)
   - ✓ Technical controls to enforce operating system password policy are in place (as per password policy)
   - ✓ Audit logging of privileged access and log-on/log-off activities are being captured (as per logical access Policy)
   - ✓ Systems are patched and up to date (both operating systems and software). All software and operating systems must be updated with the latest security patches recommended by the manufacturer. Priority should be given to the installation of those patches which solve the most serious vulnerabilities in the systems with greatest exposure and risk, taking into account criticality.
   - ✓ All software is authorized and licensed appropriately

8. To deal with security mechanisms and measures, the **Data Owner** may choose to delegate the security tasks, in full or partially, to an Asset Handler or other representative (e.g. ISS, or 3rd party security). **This delegation does not exempt the Data Owner from their responsibility and they must make sure that the delegated jobs have been carried out correctly and corrective actions taken; they remain accountable. In addition, where delegated to ISS this must be by written mutual agreement.**

5. Responsibilities

Name	Responsibility
ICT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
University Management Team	Approval of the Policy
Data Owner	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

QA401 Data Handling

QA402 Data Classification
QA404 Password Policy
QA405 Partnering Policy
QA406 Remote Access Policy
QA408 Logical Access Policy
QA409 Encryption Policy
QA410 Anti-Virus and Malware Protection Policy
QA411 End User Policy