NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: **QA408**
Title: **Logical Access Policy**
Review Date: **September 2020**
Approval: **University Management Team (UMT)**

1. Purpose

IT assets owned by NUI Galway play an important part in delivering many crucial services to NUI Galway staff and students. In order for services to continue to be delivered and expand it is important that these assets are protected by ensuring that adequate security controls are in place.

This policy details the minimum controls required in order to access a system and to ensure the correct level of access provided to the system. This includes access to all systems (including operating system, databases and applications).

2. Description

The policy applies to:

- All staff and students who have access to University IT systems
- All contractors, vendors or others (third 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 Asset Owner.

It is the personal 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 that all staff using the IT systems are aware of and understand their responsibilities as outlined in this policy.

3. Definitions

An **"Asset Owner"** (sometimes referred to as a **"Business Owner", "System Owner",** or **"Data 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 Asset 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. Requirements

The following security controls, when available, must be activated on all devices to help protect against unauthorized access or theft of sensitive NUI Galway information contained on the device:

1. Access to systems & data must be protected by a username and password.

2. All user accounts must be assigned a unique identifier based on the user's name. Generic accounts must not be used for individual access to systems or devices e.g. "admin", "helpdesk", etc. There will be no anonymous guest accounts on any critical systems which would enable access to personal sensitive data.

3. Users of systems must ensure they understand and are compliant with the University End User Policy.

4. User and group permissions should be allocated on an as-required basis. If a user/group does not need access to a particular set of data or functions they should not be granted the access (regardless of their level of authority).

5. Access to devices must be based on "minimum rights" basis. For example, a user who requires to perform a simple non-privilege task (e.g. view logs), should not be given permissions to perform privileged tasks.

6. Authorisation should be granted based on access profiles and groups and never to individuals.

7. Asset Owners are responsible for ensuring that appropriate security measures are in place relative to the information and classification of the asset.

8. Access to systems and devices must be reviewed on a regular basis as defined by that **Asset Owner**. The review process must include:

- The revision of the lists of users with access to the system
- Revision of the roles and associated permissions to ensure segregation of duty?
- Approval of the list by the Asset Owner by correlating with actual requirements.
- Removal of all incorrectly defined, unauthorised or redundant accounts.
- Retention of auditable review results, evidence of completion and supporting communications for at least two iterations.

9. All accesses to systems, databases and applications must be fully accountable and auditable in an audit trail.

10. All operating systems, databases or other systems/application must conform to a documented standard. At a minimum, this includes:

- All non-essential programs or services must be shut down or disabled
- All security patches recommended by the vendor should be reviewed and installed as deemed necessary and in line with security requirements.
- Default systems accounts must be removed, locked, or have their name and password changed.
- Default access methods (for example - SNMP with default community strings), must be disabled or appropriately secured in line with password policy.
- Systems are restricted from booting to removable media?
- NUI Galway Password Policy must be enforced on the system.

11. All System and application logins should display a legal banner prior to the authentication process.

The purpose of a legal banner is to:

- Provide Legal Protection should evidence need to be collected from a device.
- Shield administrators from prosecution
- Acts as a deterrent to potential intruders.

This banner should be displayed prior to login, and must include:

> WARNING: To access this system you need prior authorisation and you are strictly limited to the use indicated therein. Non-authorised access to this system or its improper use is not allowed and goes against the Corporate Security Policy and current legislation. The use you make of this system may be monitored.

The legal banner must not contain:

- Any non-public information
- Mention of the purpose, location or owner of the device or any other identification information.
- It should not say "Welcome" anywhere in the description.

The above banner should be displayed on all interfaces to both the system and applications prior to authentication.

12. Password failure messages should use a generic login failure response which does not disclose existence or non-existence of a username.

13. After a number of consecutive failed authentication attempts, the account must be locked out to prevent brute-force password attempts in line with the password policy.

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
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 Policy
QA402 Data Classification Policy
QA404 Password Policy
QA406 Remote Access Policy