NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA406

Title: Remote Access Policy

Review Date: September 2020

Approval: University Management Team (UMT)

1. Purpose

Remote access to NUI Galway systems will be required for a variety of purposes. This remote access must be controlled to ensure that NUI Galway's systems and data are not placed in jeopardy. The purpose of this policy is to ensure the correct balance between access and the potential risk posed to systems and data, and to ensure the continued availability and confidentiality of these systems and data.

Special security issues that relate to mobile devices include the following:

- Any malware (viruses, worms, Trojans) that infect the device can bypass the University's security and spread rapidly to other devices connected to the network;
- Unauthorised access to any sensitive data stored on a NUI Galway systems through the mobile device and the potential for that data to be stolen or lost;
- Use of personal devices to access/store University systems and data.

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.

3. Definitions

"Remote Access" is defined as access to NUI Galway's systems from any non-campus network or from the Internet whether on or off campus.

"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

1. All access to the NUI Galway network, applications, and/or data is subject to the NUI Galway Policy Rules and Regulations and in particular to NUI Galway ICT Policies, e.g. Data Protection, Data Handling, Data Classification, Encryption Policy, End User Policy.

2. Remote access to NUI Galway systems must be for a specified and legitimate purpose.

3. Remote access to the university must use an approved remote access technology. Current approved remote access technologies are:

a. ISS approved University Virtual Private Network (VPN)

b. Direct SSH Access to an individual host

c. Remote Applications published by ISS

d. Microsoft Windows Virtual Desktop

If the remote access mechanism is not detailed above then it is not an approved method and should not be used**. This includes all other forms of remote access. Specifically software which establishes outbound connection to 3rd party sites, and can then be used to access a user's desktop remotely must not be used without prior specific approval by the IT Security Officer. In the event of any doubt as to the application of this clause, the guidance of ISS should be sought.**

4. The same security policies apply to remote workers as would to office based personnel. When working remotely all applicable policies and in particular security policies must be complied with. For example if working on "NUIG Galway Restricted" information, all paper waste must be disposed of properly and in accordance with the Data Classification and Handling Policy.

5. All individuals are responsible for safeguarding the remote access credentials granted to them and making sure that unauthorised individuals do not use them. These credentials may consist of username and password combinations, authenticators for Multi Factor Authentication, digital certificates or other software or hardware. Users must not provide their password to any other person or entity.

6. If you remotely use NUI Galway systems then you must ensure that the following are in place:

- The ability to use Multi Factor Authentication where enabled
- A strong password which conforms to NUI Galway's password policy.
- You must not attempt to log on as another individual even if they have given you credentials.
- No group (or generic) accounts are used for remote access.
- The system you are using for remote access has sufficient protection in terms of antivirus, malware protection and operating system patches.
- Caution should be exercised when accessing NUI Galway systems remotely and that they are not accessed from networks that may be insecure.

7. Remote users must not bypass security mechanisms to remain logged onto systems for longer periods.

8. When remote access is provided to any system, access should be granted on the principle of "least-privilege". Specifically, users should not be granted access to systems or functions to which they do not need access.

9. Sensitive information must not be stored on Smartphones (or other mobile devices) or must be protected in accordance with NUI Galway's Data Classification and Data Handling policies. At a minimum access to the mobile device must be protected (e.g. via passcode or fingerprint).

10. Any suspicious behaviour or security incidents (such as comprise of your network account) must be reported to NUI Galway Information Solutions and Services (ISS) Helpdesk and to your Head of School or Unit.

5. Responsibilities

Name	Responsibility
ÌCT 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 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

QA405 Partnering Policy

QA407 IT-Asset Protection Policy

QA408 Logical Access Policy

QA409 Encryption Policy

QA410 Anti-Virus and Malware Protection Policy

QA411 End User Policy