NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA410

Title: Anti-Virus and Malware Protection Policy

Review Date: September 2020

Approval: University Management Team (UMT)

1. Purpose

The purpose of the Anti-Virus and Malware Protection Policy is to establish principles which must be met to prevent malware from entering the university environment, to identify and report on malware or suspected malware attacks, and to define appropriate actions to eliminate and recover from malware related incidents.

2. Description

This policy applies to all NUI Galway employees and students using the university resources. It is the personal responsibility of each individual to take precautions to ensure that all forms of malware are not introduced into any university resources or system with which they come into contact. Further information and training is available on the ISS website: https://www.nuigalway.ie/itsecurity/

Any other parties, who use, work on, or provide services involving NUI Galway computers and technology systems will also be subject to the provisions of this policy.

3. Definitions

For the purposes of this policy, we apply the term **"malware"** to define all types of "**mal**icious soft**ware**" that performs malicious tasks like deleting files, changing computer settings, collecting personal information, gaining access to systems, holding the user to ransom etc. This includes virus, worms, trojans, rootkits, keyloggers, spyware, adware, phishing etc.

"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 requirements apply:

1. All users must note and report any observed malware or suspected security incidents as soon as possible. Particularly virus outbreaks must be reported to NUI Galway Information Solutions and Services (ISS) and to your Head of School or Unit.

2. All end-user devices connecting to university resources should have appropriate anti-virus and malware protection installed and active.

To protect against malware infections, an 'in-depth defence' strategy is required to minimise the risk of loss or damage to services. This includes anti-malware security controls at:

- Client Protection
- Network Perimeter
- Server Level

Client Protection

3. All PCs and laptop equipment must have anti-virus software installed and active.

4. All PCs and laptop equipment must have on-line (real-time) scanning enabled and enforced as a background service (i.e. each file access must be checked while loading).

5. All PCs and laptop equipment should have a minimum weekly scan of all files for malicious code.

6. All PCs and laptops must have automated update mechanisms enabled and active to ensure they are provisioned with the latest virus signature files. This is ensured by installation of the McAfee ePolicy Orchestrator Agent (EPO agent) from the ISS website: https://www.nuigalway.ie/itsecurity/anti-virus/

For additional information on anti-virus software which is available to staff and students go to the ISS Webpages: https://www.nuigalway.ie/itsecurity/anti-virus/

Server Protection

7. All Microsoft based Servers must have anti-virus software installed and active. This includes:

    a. Real-time "on-access" scanning.

    b. Weekly scan for malicious code.

8. All anti-virus software must be configured to be updated automatically. The Virus Signatures should be updated (at a minimum):

    a. Daily for servers with network access to virus signature update server

    b. Weekly for other non-network connected servers

9. Due to the fundamental different approach used for security on UNIX based (UNIX & LINUX) system including UNIX file system security, User permissions, and executable not depending upon extension, it is not a requirement that UNIX systems have anti-malware installed and active. However, UNIX based systems are not bulletproof and can still suffer from malware and Trojans and it is therefore recommended that critical systems, or systems that perform a high level of interactivity with users should have anti-malware protection installed and active Network Perimeter Protection

10. Approved anti-malware solutions must be deployed at all internet and e-mail gateways to prevent malware from entering the network.

11. Email checking for malware must be performed at the e-mail gateway for both incoming and outgoing messages.

Compliance with Policy

The University reserves the right to disconnect any device from the network if an infection is found or suspected. The machine will remain disconnected until the infection is removed.

Individuals may be subject to disciplinary action if this Policy is breached.

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

QA411 End User Policy

QA398 Personally Owned Digital Devices (BYOD) Policy