NUI Galway
OÉ Gaillimh

Policies and Procedures

Code: QA409

Title: Encryption Policy

Review Date: September 2020

Approval: University Management Team (UMT)

1. Purpose

As per the Data Classification Policy, there are two types of information processed by NUI Galway, notably:

- **Public Information** intended for general public use and would cause no harm to any individual, group, or to the University if made public.

- **Classified Information** which refers to all other types of information processed within NUI Galway. This includes all forms of data which if lost would be expected to have adverse effect on the university operations, assets or individuals. This also includes research related data.

The purpose of the Encryption Policy is to establish principles to effectively and efficiently plan, prepare and deploy appropriate encryption solutions in order to secure NUI Galway classified information in line with NUI Galway Data Classifications and Handling Rules (see related documents below), and specifically where encryption is mandated.

2. Description

The Data Classifications Policy defines **Classified Information** within **NUI Galway** as one of **NUI Galway Controlled, NUI Galway Restricted and NUI Galway Highly Restricted** classifications. The Data Handling policy defines the handling rules for each classification type and when encryption is mandated for electronic storage, and transfer to internal and/or external to NUI Galway.

This policy applies to:

- All Faculty, Staff, Research and Students who have access to University IT Systems

- All contractors, vendors or others (including 3rd parties), who have access to University IT Systems.

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 all staff using the IT systems are aware of and understand their responsibilities in this policy.

3. Definitions

Classified Information refers to all information classified as one of:

NUI Galway Controlled

NUI Galway Restricted

“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. If NUI Galway classified information is transferred or stored internal or externally to NUI Galway it must be encrypted where mandated by the data handling rules. This applies to all types of storage and transfer including laptops, PC, mobile devices/smartphones, external drives, backup tapes, storage media etc.

2. Schools, departments and business functions are required to employ University-approved encryption solutions for this purpose. This applies to both University owned and privately owned devices (BYOD). While privately owned devices (laptops, external drives, smartphones etc.) may be utilised to process NUI Galway classified information, the necessary encryption must be installed and appropriate security enforced on the device regardless of the ownership of the device. If this is not desired then you should not store NUI Galway classified information on a personal device.

3. Valid Encryption Methods are as follows:

Full Disk Encryption

Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area.

E-mail Encryption

E-mail-specific products integrate encryption into the e-mail client, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular encryption of e-mail communications. Most departments can make use of a broader range of file/folder encryption products to encrypt individual files and folders. Where any classified data is transmitted via attachment to an email outside the NUIGalway.ie domain it should be separately encrypted and password protected.

External Devices Encryption

External devices such as hard drive can be encrypted in their entirety. Data on these systems can be considered secure without access to the key and encryption software.

Portable Storage

Portable storage capability such as DVD's, CD's and USB flash drives should not be utilised for classified data storage or transfer, even in an encrypted format.

File/Folder Encryption

Individual or multiple files or folders can be encrypted separate from the host operating system. These encrypted archives can be stored in different locations such as network shares, external hard drives or be transmitted securely via e-mail. This is prone to error, and where classified information is stored on the device preference is to use Full Disk Encryption.

Mobile Device Encryption

Mobile devices such as PDAs and smartphones allow users to exchange, transfer and store information from outside of the university. The extreme portability of these devices renders them susceptible to theft or loss. ISS recommends the use of standardised devices such as laptops for storing, transmitting or processing NUI Galway Highly Restricted Data.

Transport-Level Encryption

Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient in order to ensure delivery without eavesdropping, interception or forgery. This scenario requires the appropriate configuration of a server in order to allow clients to connect in a secure manner.

For applicable and preferred products for each encryption method please refer to ISS website.

4. Passwords or encryption keys required to open encrypted files must be supplied to authorised personnel on request (if stored on the file system in encrypted format). All encryption key passwords should be stored securely in case required to reproduce the files.

5. All passwords stored electronically must be encrypted. The encryption algorithm should utilise a one-way approved salted hashing algorithm. Passwords must not be saved in clear text on a file or database for any purpose.

6. Where password-based encryption is used, the password must never be transmitted in the same way as the encrypted file. For example, if an encrypted file is e-mailed, the password should be sent by another means such as SMS message.

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

QA401 Data Handling

QA402 Data Classification

QA404 Password Policy