Letterkenny Institute of Technology

Encryption Protection Standard

Version 1.1

Document Location

This document will be stored on the staff Intranet server. Master and hard copy will be held by the IT Manager.

Revision History

Date of this revision: 01/10/2018	**Date of next review:** 01/10/2019

Revision Number	Revision Date	Summary of Changes	Changes marked
1	01/12/2013	First Version	
1.1	3/12/2018	Addition of new open source encryption\Windows 10	

Approval

This document requires the following approvals:

Title	Date
IT Manager	October 18
Vice President for Academic Affairs and Registrar	October 18

This Encryption Protection Standard will be reviewed on a periodic basis.

Table of Contents

1. PURPOSE

The purpose of this Encryption Protection Standard is to provide specific guidance to Letterkenny Institute of Technology (LYIT) staff in relation to using encryption technology to protect data stored or data transmitted electronically. This standard should be read in conjunction with Letterkenny Institute of Technology's Information Security Policy.

2. DEFINITIONS

Encryption: is the conversion of data into a form called cipher text that cannot be easily understood by unauthorised people. The purpose of encryption is to protect confidential or personal information during transmission over the network or unauthorised access in the event a portable device or removable media is lost or stolen.

Decryption: is the process of converting encrypted data back into its original form, so it can be understood by authorised people.

Removal Media: refers to storage media which is designed to be removed from workstations easily. Examples of removable media commonly include: USB flash drives, external hard drives, optical disks (DVDs, CDs, and Blu-Ray discs), floppy disks, magnetic tape, portable music, cameras or smartphone device.

Portable Devices: refers to laptops, netbooks, tablets, mobile smartphones and E-book readers.

Personal Data: according to the Data Protection Acts 1988-2003, personal data is data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of a data controller. Letterkenny Institute of Technology are both the data controller and data processer in relation to student and staff data. Examples of personal data are student exam results, student assignments, staff resumes.

Confidential Data: is data that should not be available or accessible to the public. Such data may include financial, commercial, research, and Intellectual property data. The unauthorised or accidental disclosure of this data could seriously and adversely impact LYIT.

Transmission: is the process of sending something (information or otherwise) from one location to another location.

Passphrase: A passphrase is a short phase or sentence of 16 characters or more (which may include spaces) now commonly used as a secure password.

Strong Password: A strong password consists of at least eight characters that are a combination of letters, numbers and symbols (@, $, %, etc.).

Trusted Platform Module (TPM): is a hardware chip built into newer laptops to store passwords, encryption keys, and digital certificates. Storing this authentication data on the chip, instead of on a computer hard drive, increases the security of encrypted data.

3. ROLES AND RESPONSIBILITIES

Staff

- To ensure that they follow the Encryption Protection Standard when storing personal data or confidential LYIT data outside the Institute's secure network storage.
- To ensure that they follow the Encryption Protection Standard when transmitting personal data or confidential LYIT data over the un-secure data network such as the Internet.
- To report any breaches of this standard to the Data Protection Officer for the transmission or storage of personal data.

Computer Services Staff

- To provide guidance to LYIT staff on the use of encryption technology.

IT Manager

- To monitor compliance with the Encryption Protection standard.
- To inform the Registrar of suspected non-compliance and/or suspected breaches of the Encryption Protection standard.

4. SCOPE

This document outlines the general guidelines to be followed by LYIT staff in terms of encryption protection standards.

5. ENCRYPTION PROTECTION STANDARD

5.1 STORAGE ENCRYPTION

Best practice is for electronic information to reside on secure Institute servers. When it is absolutely necessary to store personal or confidential data on removal media or portable devices then encryption is required. Any personal or confidential data should be only stored on removal media or portable device for a short period of time and deleted when no longer needed on the device. The following safeguards are required to be adhere to when storing electronic documentation (personal or confidential data):

REMOVABLE MEDIA

- Optical storage (CD/DVD/Blue-ray) shall not be used to store electronic documents that is deemed to be personal data or confidential data.
- Only use hardware encrypted USB pen drives, known products in LYIT include, but not limited to are Integral Crypto Drive , IronKey, Kingston Data Traveler 4000 managed and Kanguru Defender 2000.
- Only use hardware encrypted external hard drives, known products in LYIT include, but not limited to are, Western Digital MyPassport portable hard drive.

- In circumstances where hardware encryption devices are not available, then it is recommended to use software encryption tools such as Microsoft BitLocker (only available in Window 10 Professional\Enterprise) or VeraCrypt (open source\free tool). Guidance documents on how to encrypt using VeraCrypt is available on our Intranet site (https://intranet.lyit.ie).

PORTABLE DEVICES

- All TPM supported laptops issued to staff are encrypted by default using Microsoft Windows BitLocker.
- Authorised staff who are storing any personal data or confidential data on their Institute laptop device should contact Computer Services Helpdesk to confirm if their device is BitLocker enabled.
- Guidance documents on how to encrypt tablets and smartphones are available on the Intranet site or available (https://intranet.lyit.ie).

5.2 E-EMAIL FILE TRANSMISSION ENCRYPTION

In order to protect personal or confidential data been transmitted using e-mail then the following safeguards are required to be adhere to when transmitting electronic documentation:

- Compress files .zip or zipx formats using 7Zip, WinZip, or equivalent product using the 256-bit Advance Encryption Standard (AES) features **or**
- Encrypt the document (Microsoft Word, Excel, PowerPoint and Adobe Acrobat) using the built in encryption features within Microsoft Office or Adobe PDF reader.
- Ensure a strong password or pass phrase is generate to encrypt the file.
- Communicate the password or pass phrase via a telephone call to your recipient. Do **not** provide the password or pass phrase by e-mail.

Please remember, while attachment is encrypted, the content of the e-mail message will not be encrypted so it is important that any sensitive or confidential information be contained in the attachment (encrypted document).

Refer to our user guides for instruction on how to encrypt files, guidelines documents available on the Intranet site (https://intranet.lyit.ie).

5.3 SECURE COMMUNICATION

Any LYIT information Systems are Services which have the potential to communicate personal data over un-secured data communication networks such as the Internet, shall use cryptographic protocols that provide security for communication over networks e.g. TLS or SSL.

Authorised staff who is required to transmit personal or confidential data over un-secured data communication networks such as the Internet to Institute approved 3rd parties must ensure that cryptographic protocols are used to secure the communication e.g. web page uses SSL (https://upload.lyit.ie) or using secure File Transfer Protocol (SFTP), etc.

Staff needing to send large files securely should use HEAnet's File Sender services. File Sender can be accessed at https://filesender.lyit.ie . Please ensure you select the encryption option when sending files through File Sender.

Staff should seek advice from the Computer Services Department to confirm if transmission of confidential or personal data over the network conforms to the required security protocol.

Please note the following:

- Staff should never use the Institute's public folder system (Y Drive) for storing any personal or confidential data. The public folder system is an unsecure file share system, accessible to all staff and students.
- Staff should never use "cloud" storage services for personal or confidential data as this places information at risk and can place information outside European legal jurisdictions. Examples of cloud storage services include: Dropbox, GoogleDocs, OneDrive, etc.
- Staff should not store personal or confidential data on non-secure removable media.
- Any portable device that is storing personal or confidential data must employ full disk encryption using approved encryption.
- Staff should not transmit personal or confidential data over the Internet without using encryption and verifying the receiver of the information.
- Staff should not store or transmit personal data without authorised permission from the Data Controller (Contact: Data Protection Office for further information).
- If you forget the password to any files encrypted, there is no option to recover it.