lyit | Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Letterkenny Institute of Technology

Information Security Policy

Final Version 1.1

September 2018

Table of Contents

Revision History

Date of this revision: 08th December 2017		**Date of next review:** 1 January 2019
Version Number/Revision Number	**Revision Date**	**Summary of Changes**
1.0	31/01/2013	First draft.
1.1	15/12/2015	Amendments proposed by TUI

Document Location

Website – Intranet	x
Website – Staff Hub	x
Website – Student Hub	x
Other:	

Consultation History

Version Number/Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
1.0	31/01/2014	HR	Draft forwarded to HR
1.0	31/03/2015	Unions	Forwarded to unions via HR Office
1.1	1/1/2017	Union	Agreement with unions

Approval

This document requires the following approvals:

Title	**Date**
Executive Board	10 December 2017
Governing Body	13 December 2017

This policy shall be reviewed and updated annually.

1. PURPOSE

Letterkenny Institute of Technology (LYIT) information systems underpin all of the Institute's activities, and are essential to its teaching, learning, research and administrative functions. Security of information must therefore be an integral part of the Institute's operation and structure to ensure continuity of business, legal compliance and to protect LYIT from financial and reputational loss.

The purpose of this document is to set direction for information security management within LYIT. The policy sets out the overall approach to information security and provides a security model aimed at:

- Implementing best practices to protect information assets from unauthorized use, disclosure, modification, damage or loss.
- Protecting the work and study environment of staff and students and the good name and reputation of LYIT.

LYIT information security policy should be read in conjunction with relevant standards, procedures and guidelines which support the implementation of this policy (Refer to Section 5).

2. DEFINITONS

Information Security – According to the ISO 27002 standard defines information security as the preservation of confidentiality, integrity and availability of information.

Confidentiality – Confidentiality restricts information access to authorised users.

Integrity – Integrity protects the accuracy and completeness of information through the controlling of information modifications.

Availability – Availability ensures the information is accessible when needed.

Information Asset –The ISO 27002 Standard defines an asset as anything that has a value to an organisation. Information has value and is classified as an asset. Information refers to data that is processed but also encompasses unprocessed data that is stored on LYIT Information Technology (IT) resources.

Content - Content is information with relevant metadata that has a specific use or is used for a particular business purpose.

Records – ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Information Technology (IT) Resource – All IT systems owned, held under licence or otherwise controlled by LYIT including but without limitation to:

- Workstations including desktop PCs and laptops;
- Servers;
- Network technologies such as routers (WAN, LAN and wireless) and associated media and systems;
- Printers;
- Phones, Smart Phones, tablets and other portable ICT devices;
- USB and all portable memory devices;
- All other media and devices provided by LYIT;

- All other media and devices used to access LYIT Information Assets.

Sensitive 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. LYIT are both the data controller and data processer in relation to student and staff data.

Refer also to definitions per Section 2.0 of the IT Documentation Framework.

3. ROLES AND RESPONSIBILITES

The following roles and responsibilities apply in relation to this Policy:

Governing Body:

- To review and approve the policy on a periodic basis

Registrar and Secretary / Financial Controller:

- To ensure the Policy is reviewed and approved by the Governing Body.
- To consult as appropriate with other members of the Executive and Management Teams.
- To liaise with Human Resources (HR) or Secretary/Financial Controller office on information received in relation to potential breaches of the Policy.
- To ensure the appropriate standards and procedures are in place to support the Policy.

IT Manager:

- To define and implement standards and procedures which enforce the Policy.
- To oversee, in conjunction with Data Owners, compliance with the policy and supporting standards and procedures.
- To inform the Registrar's Office of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

HR Office and Secretary / Financial Controller Office

- To follow relevant and agreed disciplinary procedures when HR or Secretary / Financial Controller's office is informed of a potential breach of the Policy (Refer to Section 7).
- To manage the disciplinary process.

Staff/Students/External Parties:

- To adhere to policy statements in this document.
- To report suspected breaches of policy to their Head of Department or the IT Manager.

If you have any queries on the contents of this Policy, please contact the Registrar or the IT Manager.

4. SCOPE

This Information Security Policy covers security of:

- LYIT Information Assets;
- LYIT IT Resources.

This policy applies but is not limited to the following, LYIT related groups as defined in Section 3.0 of the IT Documentation Framework:

- LYIT staff;
- LYIT students;
- LYIT external parties.

Based on the definition of Information Security in section 2, this policy outlines key policy statements relating to these areas.

5. SUPPORTING DOCUMENTS

- LYIT IT Documentation framework;
- LYIT Acceptable Usage policy;
- LYIT Data Governance policy;
- LYIT Password standard;
- LYIT User Administration procedure;
- LYIT Anti-Virus Scanning and Protection standard;
- LYIT Encryption Protection standard;
- LYIT Portable Device Security procedure;
- LYIT Client Configuration procedure;
- LYIT Server Configuration procedure;
- LYIT Physical Access procedure;
- LYIT Disaster Recovery Plan.

The above list is not exhaustive and other LYIT documents may also be relevant.

CONFIDENTIALITY

LYIT and all staff, students, and external parties of the LYIT community are obligated to respect the rights of individuals and to protect confidential data.

All LYIT information is to be treated as confidential unless otherwise indicated. When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Please refer to LYIT's Data Governance Policy.

Access to information is granted on a needs only basis (Refer to LYIT User Administration Procedure); LYIT staff are granted specific access to allow them to carry out their job functions.

All information is stored in a secure manner; this may require physical and logical restrictions. At a minimum, logical security includes the use of unique identifiers and passwords which are sufficiently complex where staff, students and external parties operate in accordance with LYIT password standard.

All hardware used for the storage of LYIT data is to be purged of data and securely destroyed once it is no longer to be used.

When tapes and other secondary storage devices reach the end of their useful life they are to be purged of LYIT Data and securely destroyed.

INTEGRITY

Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.

System changes should be completed in accordance with the LYIT change management procedure with which all LYIT personnel should be familiar.

An appropriate audit trail including database logs of the creation, amendment and deletion of LYIT data and/or systems is maintained by LYIT. This is particularly important in relation to the following:

- Data including details on staff, students and suppliers;
- Data including inward fee payments, outward supplier payments, and payroll transactions;
- LYIT resource usage data;
- LYIT data which may reside outside main LYIT system(s).[1]
  Please refer to the LYIT Data Governance Policy.

AVAILABILITY

To ensure that LYIT data and resources are available when required, three key layers of control are employed:

[1] This could include data which resides on external systems or data that resides on internal such as Excel Spreadsheets, local desktop databases, etc.

- Prevention of data loss through data back-ups (Refer LYIT Data Backup and Monitoring procedure);
- Prevention of system downtime and/or unauthorised data access and amendment through anti-virus protection (Refer to LYIT Anti-Virus Scanning and Protection standard)l
- Ability to respond to events which prevent data/system access through Disaster Recovery Planning (DRP).

6. MONITORING

LYIT reserve the right to monitor all LYIT IT resources, information assets, content and data at all times. Any monitoring of LYITD data and/or LYIT information resources is to ensure the secure, efficient and effective operations. The monitoring is non-intrusive and does not involve access or reading of content.

LYIT reserve the right to log any required LYIT data concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

LYIT may also log all changes made to LYIT systems and applications.

7. VIOLATION OF POLICY

Contravention of any of the above policy will lead to the removal of LYIT resource privileges and can lead to disciplinary action in accordance with the LYIT disciplinary procedures.

Institiúid Teicneolaíochta
Leitir Ceanainn
Letterkenny Institute
of Technology

Bóthar an Chalaidh, Leitir Ceanainn
Contae Dhún na nGall, Éire

Port Road, Letterkenny
County Donegal, Ireland

Telephone + 353 74 918 6000

Fax + 353 74 918 6005

www.lyit.ie