Institiúid Teicneolaíochta Leitir Ceanainn
Letterkenny Institute of Technology

Data Access Management Policy

June 2018

Contents

Revision History

Date of this revision: 21/6/2018	Date of next review: 21/6/2019

Document Location

Website – Policies and Procedures □

Website – Staff Hub ☒

Website – Student Hub □

Other: □

Approval

This document requires the following approvals:

Name	Title	Date
HMG	Executive Board	11 June 2018
HMG	Governing Body	21 June 2018

This Policy was agreed by the Governing Body on 21 June 2018. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

1. OVERVIEW

The Institute is responsible for the processing of a significant volume of personal information across each of its Schools and Departments. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- It is the responsibility of each School and Function to ensure this personal information is processed in a manner compliant with the relevant data protection legislation and guidance.
- The Institute has an appointed Data Protection Officer ('DPO') who is available to Schools and Functions to provide guidance and advice pertaining to this requirement.
- All Staff must appropriately protect and handle information in accordance with the information's classification.
- Personal Data is considered Confidential Information and requires the greatest protection level.

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. PURPOSE

The purpose of this policy is to ensure there is a process in place to actively manage the life cycle of system and application accounts – their creation, use, dormancy, and deletion - in order to minimize opportunities for attackers to leverage them. Additionally, the purpose of this policy is to ensure there is a process and tools in place to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

3. ROLES AND RESPONSIBLITIES

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

Governing Body	To review and approve the policy on a periodic basis.
Executive Board	The Executive Board (EB) is responsible for the internal controls of LYIT, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. The EB is responsible for: • Reviewing and approving this Policy and any updates to it as recommended by the Data Protection Officer. • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility. • As part of the Institute's Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the GDPR. • Ensuring oversight of data protection issues either through their own work or a Data Protection Oversight Committee or other governance arrangement.

IT Manager	• To monitor compliance with the access management requirements outlined in Section Five of this policy. • To inform their Head of Function and Data Protection Officer of suspected non-compliance and/or suspected breaches of the access management requirements (outlined in section five).
Data Protection Officer	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to executive management.
Staff/Students/External Parties	• To adhere to policy statements in this document. • To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.

If you have any queries on the contents of this Policy, please contact the Executive Board or Data Protection Officer by email at dpo@lyit.ie.

4. SCOPE

This policy applies to:

- Any person who is employed by LYIT who receives, handles or processes data in the course of their employment.
- Any student of LYIT who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process data on behalf of LYIT.

5. POLICY

This policy should not be viewed in isolation. Rather, it should be considered as part of the LYIT's suite of Data Protection and IT policies and procedures (see Appendix A). Of particular relevance is the LYIT's User Administration Procedure.

5.1 Policy Requirements for Data Access Management

- Establish and enforce a process to ensure that access to system and hosts by all types of end-user (including Administrator end-users) accounts is restricted to ensure that only specific privileges are assigned to end-users commensurate with their role and justification.

- Configure access for all end-user accounts to systems and hosts through a centralised point of authentication, for example Active Directory or LDAP.
- Configure network and security devices for centralised authentication, for example TACACS or Radius.
- Ensure that all access privileges held by all end-user accounts has a documented and valid business justification approved by senior management.
- Establish a process to ensure that all privileges held by all end-user accounts is reviewed on a regular basis and any unauthorised access or access held without a valid business justification is remediated immediately. Access must be reviewed immediately in response to new and evolving threats, capabilities, vulnerabilities, customer requirements or experience of security incidents.
- Establish a process to ensure that all end-user accounts, two-factor authentication tokens held by terminated staff are suspended and deleted and all access to end-user accounts held by terminated staff is removed immediately. Any re-joining staff must reapply for all access and privileges to systems and hosts.
- Establish a process to ensure that access for all end-users whose role has changed is modified commensurate with their new role/duties.
- Ensure that all resources use personally identifiable accounts when access any system or host.

5.2 Policy Evidence for Data Access Management

Expected evidence to confirm the operation of this policy:

- Inventory of end-user accounts including active and disabled accounts (along with date end-user account was deactivated) (6 monthly).
- Assurance report to confirm that end-users accounts in use remain valid and that the privileges held by end-user accounts are authorised with a current legitimate business justification (6 monthly).
- Assurance report detailing actions taken and the progress against these actions to resolve access that no longer has a valid business justification for all end-user accounts (6 monthly).

5.3 Policy Requirements for Data Access Controls

- Ensure that all information stored on systems and hosts is protected with file system, network share, application, or database specific access control lists and no sensitive personal data is available to read-only authenticated end-users or world-readable.
- Ensure that archived data (which is not backup data) that is no longer required is removed from systems and hosts or ensure these systems and hosts are removed from the network when there is no longer a valid business justification to retain it. This includes, copies of business data, logs data, configurations, software, system and host device images.

5.4 Policy Evidence for Data Access Controls

Expected evidence to confirm the operation of this policy:

- Inventory of information stores containing sensitive information (including business data, configuration information, system files, log files, password files, source code, etc.) and the Access Control Lists (ACLs) applied to these information stores.
- Assurance report to confirm no sensitive information is available to read-only authenticated end-users or world-readable.
- Inventory of archive data stores containing sensitive information (including business data, configuration information, system files, log files, password files, source code, etc.) and the ACLs applied to these archived data stores (6 monthly).

- Assurance report to confirm no sensitive information is available to read-only authenticated end-users or world-readable within these archive data stores (6 monthly).

6. POLICY COMPLIANCE

6.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to LYIT and an infringement of the rights of employees or other relevant third parties.

6.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer in advance.

6.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the Institute's disciplinary procedures. Failure of a third party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the Data Protection Officer and/or IT Manager.

APPENDIX A: SUPPORTING DOCUMENTS

The below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Data Protection Policy
- Data Protection Procedures
- Data Retention Policy
- Data Governance Policy
- Information Security Policy
- Network Security Policy
- Systems Development Life Cycle Policy
- Data Handling & Clean Desk Policy
- Data Encryption & Data Anonymisation and Pseudonymisation Policy
- Privileged User Policy
- IT Architecture Security Management Policy
- Data Protection Incident Response & Breach Notification Policy

The above list is not exhaustive and other LYIT policies, procedures and standards and documents may also be relevant.

APPENDIX B: GLOSSARY OF TERMS

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	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.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title and description • Tags and categories • Who created and when • Who last modified and when • Who can access or update.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by LYIT. Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of an individual student file or HR file • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour and discipline.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.
Data	As used in this Policy shall mean information which either: • is Processed by means of equipment operating automatically in response to instructions given for that purpose • is recorded with the intention that it should be Processed by means of such equipment • is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System • does not fall within any of the above, but forms part of a Readily Accessible record. Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed. A Data

	Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within an Institute which is Processing Personal Data for the Institute as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor. It is possible for one Institute or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the Institute is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Third Party	Means an entity, whether or not affiliated with LYIT, that is in a business arrangement with LYIT by contract, or otherwise, that warrants ongoing risk management. These Third Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where LYIT has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data.
Data Subject	Refers to the individual to whom Personal Data held relates, including: employees, students, customers, suppliers.
Processing	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms 'Process' and 'Processed' should be construed accordingly.
Systems and Hosts	Means all in-scope hosts (including server, desktop, laptop, network switch, network router/gateway, printer, backup device, etc.)

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.

lyit

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