Dundalk Institute of Technology

Physical Security Access Policy

Version 1.0.1

Document Location

..\DkIT_Policy_Documents\Procedures

Revision History

Date of this revision:	Date of next revision:

Revision Number	Revision Date	Summary of Changes	Changes marked
	25/6/15	New Policy Document 2015	
	24/11/15	Review Document	
	04/09/18	Review Document wrt GDPR	

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
	05/09/18	James McCahill Loretto Gaughran	Review in relation to GDPR.
v1.0.1	01/11/18	James McCahill Michael Denihan	Review for GDPR compliance.

Approval

This document requires the following approvals:

Name	Title	Date
James McCahill	IT Strategy Manager	01/11/18
Michael Denihan	Computer Services Manager	01/11/18

This Policy shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1 Overview

The Institute is responsible for the processing of a significant volume of personal information across each of its Schools and Functions. 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.

Dundalk Institute of Technology gathers and generates large amounts of data and information of varying levels of sensitivity during the course of its operations, which is stored, retrieved and transferred using information systems. Dundalk Institute of Technology also relies on this data for the provision of internal and external services. The confidentiality, integrity and availability of this data and information are critical to the uninterrupted operations and timely provision of services. Securing and protecting this data from loss or theft is important for Dundalk Institute of Technology's information security and also for regulatory compliance.

2 Purpose

The purpose of this policy is to establish standards for securing access to server rooms /datacentres and information technology facilities at Dundalk Institute of Technology. It ensures that Dundalk Institute of Technology has sufficient organisational controls in place to become compliant with the General Data Protection Regulation. It highlights how the Institute's information assets are to be protected.

Effective implementation of this policy will minimise unauthorised access to these locations and provide more effective auditing of physical access controls by outlining:

- Procedures for granting, control, monitoring, and removal of physical access to secure areas.:-ICT facilities (server rooms, network closets etc.).
- Procedures The procedures for periodic review of the Institutes users and visitors i.e. contractors and their access rights.

3 Definitions

User	A user is an individual or group that require access to facilities in Dundalk Institute of Technology network, systems and/or applications to allow them to fulfil their job functions.
Access	Access may be the method off access to Dundalk Institute of Technology information technology facilities either by physical access or electronic access over the Internet using controlled channels.
Information Technology Facilities	All or any of the central IT facilities, local facilities, computing and network facilities, as the context requires.
IT Services	The Department which provides and manages any part of the IT facilities within Dundalk Institute of Technology.
Contractor	An external provider that provides computing and network facilities and services to the Institute. The provider may also be the asset custodian.
Secure Area's	Specific areas such as datacentres/ server rooms, IT restricted facilities and other information processing facilities and certain offices depending on criticality and risk exposure.

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

4 Roles and Responsibilities

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

Governing Body	To review and approve the policy on a periodic basis
IT Manager	• To implement physical and procedural measures to ensure compliance with the physical access policy. • To inform the Head of Function and/or Data Protection Officer of suspected non-compliance and/or suspected breaches of the physical access policy
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.
IT Department	• Is responsible for compliance with the Physical Access Policy as outlined in this document.
Network Administrator	• To coordinate access to Dundalk Institute of Technology server rooms /datacentres. • To inform the IT Manager of suspected non-compliance and/or suspected breaches of the Physical Access Policy.

If you have any queries on the contents of this Policy, please contact the Senior Leadership Team or Data Protection Officer.

5 Scope

This policy applies to:

- All physical installations of IT equipment on the DkIT campus

Deviations from this policy requires authorisation of the IT Manager.

6 Policy

This policy should not be viewed in isolation, rather, it should be considered as part of the Dundalk Institute of Technology suite of Data Protection and IT policies and procedures (see Appendix A). In particular, the Clean Desk policy should be referred to for controls required over the protection of physical data across the Institute.

6.1 Policy Requirements for Physical Security

6.1.1 Prevention of Unauthorised Physical Access

Dundalk Institute of Technology information assets and secure areas shall be secured from unauthorised physical access at all times by adhering to the following requirements:

- Specific areas such as datacentres/ server rooms, IT restricted facilities such as comms distribution facilities and wire closets, other information processing facilities and certain offices depending on criticality and risk exposure shall be categorised as "secure areas" and appropriate access control mechanisms shall be implemented, for example card/badge access, or electronic keypad.

- Dual controls for Access management to secure areas will include the implementation of the following:
    1. Electronic card management – a secure card access management system to facilitate card access to secured areas. This is to provide secure access to the control areas managed by IT Services.

    2. Logging access activity - a signed in/out sheet of authorised personnel / contractors / vendors / visitors. This should note multiple persons entering and/or leaving the secure area and for what purpose. Visitors must inform IT Services personnel prior to their departure and sign off on the activity/task carried out in the secured area.

- All datacentre/server room storage spaces are key locked.

- Physical access to all secure areas must be documented and approved.

- Access to secure areas will be granted only to the support personnel, contractors and visitors whose job responsibilities require access to that facility.

- The process for granting card and/or key access to these secure areas must include the evidenced approval of the IT Manager or a designated alternative e.g. an STO in the specific area.

- Access cards and/or keys must not be shared or loaned to others.

- Card access records and keys logs for secure areas must be kept for routine review based upon the criticality of the resources being protected.

- Access cards and/or keys that are no longer required must be returned to the IT manager to retain security of access to facilities. Cards must not be reallocated to another individual bypassing the card return process.

- Lost or stolen access cards and/or keys must be immediately reported to the IT Manager.

- Any access / changes to secure areas must have prior approval of the IT Manager or alternative designate.

- Users shall not leave laptops and other portable computing devices, unattended and in plain sight (for example, in public areas or conference rooms).

- While travelling, the Institute's assets shall not be left in plain sight. Car trunks and hotel safes must be utilised to secure assets.

- Users must log off or otherwise lock systems or initiate a password protected screensaver before leaving a workstation unattended (for example, Ctrl+Alt+Del or Windows logo key+L on Microsoft Windows systems).

- Password protected screen savers should be enabled after 15 minutes of inactivity.

- Lost or stolen personal devices (for example, tablet, smartphone) containing Institute information shall be immediately reported to the Data Protection Officer and IT Manager.

6.1.2 Monitoring of Datacentres / Server Rooms

Institute monitoring of datacentres / server rooms shall be monitored at all times by adhering to the following requirements:

- All secure areas must be physically protected in proportion to the criticality or importance of their function.

- IT Services manage card access to secure areas and will remove the card and/or key access rights of individuals that change roles within the Institute.

- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

6.1.3 Logs of Access

Logs of access shall be maintained at all times by adhering to the following requirements:

- An access log book (see Appendix A for sample template) must be maintained and documented for all secure areas.
- IT Services must review logs ,card and/or key access rights to secured areas on a bi-annual basis and remove access for individuals that no longer require access. Evidence of such a review must be maintained.

- Physical access (in conjunction with user access reviews) must be reviewed on a bi-annual basis by IT Manager , whereby a full list of authorised users with physical access to the secure areas must be reviewed for redundant/unauthorised accounts. The review must be evidenced with justification for authorisation and removal of redundant access.

6.1.4 Granting Visitor Access

The process for granting visitor access shall be evidenced at all times be adhering to the following requirement:

- All vendors, contractors or visitors' access shall be recorded in visitor log/tracking book.
- Vendors, Contractors or visitors requiring access to secure areas shall be escorted at all times by an authorized member of the staff
- Where external contractors are involved, it is recommended that such requests are completed in advance of the planned activity as part of the change management process. Advance notice of 2 working days is required to allow access.
- Once the required information has been provided to the IT Manager, the relevant access can be granted for the secure area.
- Access requests must be administered by persons responsible in the area the planned / requested work is to be carried out.
- Visitors must ensure that they present an acceptable form of identification for example driving license, business card.
- All visitors must familiarise themselves with the health and safety procedure and rules of access.
- All visitors must be accompanied at all times.
- Only authorised personnel can enter the secure areas.
- Food or drink is not allowed in the datacentre/server rooms or the staging areas.
- The datacentre/server rooms should be treated as a clean room environment and must be kept clean and tidy at all times.

6.2 Physical Access Modifications

6.2.1 Granting Visitor Access

New authorised access requests must be submitted to the IT manager for approval. Evidence of approval must be maintained.

6.2.2 Removing Visitor Access

Access removal requests must be acted upon immediately. If there is an unannounced termination of contract, staff member / support personnel leaving the necessary changes need to be implemented immediately.

7 Policy Compliance

7.1 Compliance

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

7.2 Compliance Exceptions

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

7.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, up to and including dismissal in the case of staff or expulsion in the case of students, 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.

Appendix A – Supporting Documents

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

- Data Protection Policy
- Information Security Policy
- Logical Access Management Policy
- Remote Access Management Policy
- Data Governance Policy
- Information Classification and Handling Policy
- Systems Development Life Cycle Policy (Privacy by Design by Default)
- Physical Access Policy
- Clean Desk Policy
- Privileged User Policy
- Patch Management

The above list is not exhaustive and other Dundalk Institute of Technology policies, procedures and standards and documents may also be relevant.