# Dundalk Institute of Technology

# Outsourcing/Third Party Access Policy

# Version 1.0.3

## Document Location

..\DkIT_Policy_Documents\Policies

## Revision History

| Date of this revision: | Date of next review: |
|---|---|

| Version Number/Revision Number | Revision Date | Summary of Changes | Changes marked |
|---|---|---|---|
| V1.0.0 | 20/05/13 | Version 1.0 release | |
| V1.0.1 | 07/10/15 | Annual Review of Document | |
| V1.0.2 | 11/09/18 | Review Document for GDPR | |

## Consultation History

| Version Number/Revision Number | Consultation Date | Names of Parties in Consultation | Summary of Changes |
|---|---|---|---|
| V 1.0.0 | 09/01/14 | James McCahill Peter McGrath Michael Denihan Linda Murphy Loretto Gaughran | Create Policy Document for DkIT |
| V1.0.1 | 05/01/16 | James McCahill Peter McGrath | Review |
| V1.0.2 | 11/09/18 | James McCahill Loretto Gaughran | Review Document in relation to GDPR |
| V1.0.3 | 06/11/18 | James McCahill Michael Denihan | Review policy for GDPR compliance |

## Approval

This document requires the following approvals:

| Name | Title | Date |
|---|---|---|
| Governing Body Finance and Risk Committee | M.F. 186.7 Review of IT Policies for GDPR Compliance | 12-Mar-2019 |
| Governing Body | Meeting Ref No:G.257.5 | 7-May-2019 |

This policy shall be reviewed and updated on a periodic basis in conjunction with the Dundalk Institute of Technology Compliance Policy.

# Contents

# 1 Overview

Third-party commercial service provider may need to have access to specific systems and services on the Dundalk Institute of Technology network to ensure that they can deliver on maintenance and services as contracted by the institute.

# 2 Purpose

The purpose of this policy is to provide direction on:

- The minimum documentation (agreements) Dundalk Institute of Technology third parties must have in place prior to outsourced arrangements being finalised with them.
- The minimum-security controls Dundalk Institute of Technology third parties must have in place prior to being granted access to Dundalk Institute of Technology electronic resources and data. The level of control required is dependent on the nature of the outsourced arrangement and compliance with GDPR.

# 3 Definitions

**Outsourcing**

Involves transferring responsibility for performing an activity (previously carried out internally with the Institute) to an external third party.

Refer also to Section 2.0 of the IT Documentation Framework.

# 4 Roles and Responsibilities

All Dundalk Institute of Technology data remains the sole property of Dundalk Institute of Technology, and therefore Dundalk Institute of Technology retains data ownership responsibilities as per GDPR requirements. Refer to Dundalk Institute of Technology Data Governance Policy for information covered by this policy

It is the responsibility of all third-parties to whom activities have been outsourced to ensure they are familiar with the contents of this policy, all contracts and agreements, and all supporting documents as per section 6 and are complying with same.

It is the responsibility of the relevant data owners to ensure that appropriate contracts and agreements are in place and to schedule formal periodic reviews of third-party compliance with this policy.

It is the responsibility of data owners, in conjunction with IT, to implement appropriate oversight of third-party activity.

# 5 Scope

This Outsourcing/Third Party Access policy covers the outsourcing of any Institute related activity or process and all third-party access to:

- Dundalk Institute of Technology data
- Dundalk Institute of Technology resources

Outsourcing providers/third parties include but are not limited to:

- Hardware and software support and maintenance staff;
- External consultants and contractors;
- IT or business process outsourcing firms;
- IT Service Providers;
- Temporary staff.



# 6 Supporting Documents

- Dundalk Institute of Technology IT Documentation Framework;
- Dundalk Institute of Technology Information Security Policy;
- Dundalk Institute of Technology Acceptable Usage Policy;
- Dundalk Institute of Technology Compliance Policy;
- Dundalk Institute of Technology Data Governance Policy;
- Dundalk Institute of Technology Data Protection Policy;
- Dundalk Institute of Technology Password Standard;
- Dundalk Institute of Technology User Administration Procedure;
- Dundalk Institute of Technology Change Control Procedure;
- HEAnet Acceptable Usage Policy – www.heanet.ie/about/aup

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

# 7 Outsourcing – Minimum Documentation / Agreements

**Contracts**

A formal contract between Dundalk Institute of Technology and the outsourcer/third party must exist to protect both parties. The contract must clearly define the types of information exchanged and the purpose for doing so.

The contract must clearly define each party's responsibilities towards the other by defining:

- The parties to the contract;
- The effective date & duration;
- The functions/services being provided (refer to service level agreement below);
- The liabilities; penalties and

- The limitations on use of sub-contractors and other commercial /legal matters normal to any contract;
- The additional controls that will be embedded or referenced within the contract – such as, legal, regulatory and other third-party obligations;
- The right of Dundalk Institute of Technology to monitor all access to and use of Dundalk Institute of Technology facilities, network systems and to audit the outsourcer's compliance with the contract;
- The right of Dundalk Institute of Technology to access and audit the outsourcer's control environment;
- Service levels, outages, service interruptions and changes to service
- Payment schedules
- Supervision of the services provided
- A dispute resolution procedure including options for mediation or other interventions;
- The primary contractor and relevant sub-contractors.
- Intellectual Property Rights
- Termination, the possible exit strategy in the event of contract termination
- Effect of Termination – the activities & actions that are agreed in advance should a termination be carried out. Data transfer/ migration costs of such activity.
- If required data transfer rates between sites / service provider and competitor sites
- Contract novation – in the event of service provider / customer being merged / demerged from parent
- Confidentiality
- Force Majeure
- Responsibilities under Data Protection legislation
- Equipment- Establish Equipment replenishment processes to ensure that the business can provide an effective service operation.

**SLA**

Following on from the contract, a clear and un-ambiguous service level agreement must be agreed which will be reviewed annually or as per agreement. Performance against SLA should be reviewed annually/as agreed.

The service level agreement must indicate the frequency of service level review meetings.

The service level agreement must indicate the consequence of non-adherence to agreed service levels.

Factors for SLA are:

- Equipment replenishment
- Support Issues regarding service levels

**Confidentiality Agreement**

If the information being exchanged between Dundalk Institute of Technology and the outsourcer/third party is sensitive information, a binding confidentiality agreement must be in place between Dundalk Institute of Technology and the outsourcer/third party, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract negotiated).

Information must be classified and controlled in accordance with Dundalk Institute of Technology Data Governance Policy and GDPR requirements.

Any information received by Dundalk Institute of Technology from the outsourcer/third party which is bound by the contact or confidentiality agreement must be protected by appropriate classification and labelling and subsequent handling.

Upon termination of the contract, the confidentiality arrangements must be revisited to determine whether confidentiality has to be extended beyond the tenure of the contact.

**Contract Termination**

This section covers activities that may have to be considered /carried out where a contract is terminated by either party and relates to the access / transfer / confidentiality of the data on third party systems.

Termination clause may include factors concerning

- Change of corporate strategy
- Voluntary exit
- Litigious exit
- Successor

# 8 Third Party Access – Minimum Security Controls

To ensure the secure handling, processing and storage of Dundalk Institute of Technology information assets by the outsourcer/third party or sub-contractors, suitable security and access controls are required to be implemented by them.

At a minimum, logical security related controls shall include but are not limited to:

- Documented Information Security Policy and procedures which are available for review and audit;
- User identification and authentication techniques including strong passwords;
- Authorization and granting of system access on a need only basis;
- Appropriate and timely review and removal of user access;
- Data encryption of sensitive data;
- Appropriate audit logging of third-party activity

At a minimum, physical security related controls shall include but are not limited to:

- Layered access controls covering perimeter and internal barriers;
- Soundly-constructed facilities;
- Physical locks/access keys;
- Access logging using automated key cards, visitor registration.

At a minimum, environment related controls shall include but are not limited to:

- Fire detection and Suppression
- Temperature and water monitoring
- Uninterrupted power supply and Generator

And finally; a Business Continuity Plan detailing business recovery operations, this will also include data backup and disaster recovery plans.

# 9 Policy Violation

Contravention of any of the above policy will lead to the removal of the third-party access and/or termination of contractual arrangements.