Dundalk Institute of Technology

Remote Access Policy

v1.0.3

Document Location

..\DkIT_Policy_Documents\Policies

Revision History

Date of this revision: 05/09/18	Date of next revision:

Revision Number	Revision Date	Summary of Changes	Changes marked
V1.0.0	20/07/15	Create Remote Access Policy	
V1.0.2	25/04/18	Review document for GDPR go-live on 25-May-2018	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
v1.0.0	10/09/15	James McCahill Peter McGrath Michael Denihan	Present Policy Document for discussion
v1.0.1	18/11/15		Present for approval
v1.0.2	05/09/18	James McCahill Loretto Gaughran	Review document for GDPR
V1.0.3	01/11/18	James McCahill Michael Denihan	Review Document

Approval

This document requires the following approvals:

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

This Remote Access Policy will be reviewed on a periodic basis.

Table of Contents

Overview

The Institute is responsible for the provision of services to its staff and students on and off campus.

To make this possible it must provide remote access to its user base and contactors to provide effective management of its IT infrastructure and services to its user base with security and data protection compliance in mind.

Purpose

The purpose of this Remote Access Policy is to review, evaluate and effectively plan for the deployment of remote access services for DkIT staff and student users and External service providers.

To ensure the security of our network and to protect the Institutes data Dundalk IT must ensure that user access is managed and controlled to all of its IT resources. This management covers on-campus access (covers user owned mobile devices) and remote access external to the campus environment. This document covers remote access provisions.

Dundalk IT must ensure that all necessary security patches are installed in a timely manner to secure the IT environment to provide proper remote access activities to Dundalk hosted / delivered services.

Definitions

Certificates -Digitally signed certificates that create encrypted connections between user's mobile device and Institute servers

Contractor

An individual or commercial company that may have been contracted by DkIT to provide goods and/or services information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, etc.) to Dundalk Institute of Technology

Mobile Device-Any mobile / portable device that is used to access Dundalk IT Resources. This can include Laptops / Tablets / smartphones. In the case of remote access this could also cover a users' privately-owned personal computer.

Network Devices- Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a firewall, core / edge switches, etc.

Network Infrastructure -Includes servers, network devices, and any other back-office equipment

Remote Access- is defined as access to Dundalk IT systems from any non-campus network or from the Internet whether on or off campus.

Risk Assessment–An evaluation of the level of exposure that providing remote access services to a network device under the Remote Access policy agreement.

Vendor -Any organisation or individual(s) that do business with the Institute

In summary, Remote Access policy is the process by which external / remote access to application software is managed in order to ensure stability and security for Dundalk IT's systems and its data security.

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 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 Vice President for Financial and Corporate Affairs and Data Protection Officer of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
Computer Services Staff	Computer Services Staff are responsible for ensuring that information resources are maintained in compliance with Remote Access policies and procedures.
Senior Technical Officers	The Senior Technical Officers within the Computer Services Department are responsible for auditing activities in their area of responsibility.
Non-Computer Services IT systems	Administrators of systems not managed by Computer Services are responsible for ensuring that their systems operate in compliance with the DkIT Remote Access policies and procedures (e.g.: departmental servers, utilities devices, etc.).
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.

Scope

This policy applies to:

- Dundalk Institute of Technology staff
- Dundalk Institute of Technology students
- Dundalk Institute of Technology external parties

Remote Access Policy

Remote access connections must be strictly controlled and only granted to users that meet at least one of the following criteria:

1) DkIT staff, students, guests or contractors who have been approved by DkIT to work offsite.
2) DkIT staff, students, guests or contractors whose role requires them to spend a considerable amount of their time out of the office or workplace.
3) DKIT staff, students, guests or contractors who are responsible for administration, support or maintenance of the DkIT network and/or information systems.
4) Third party commercial service providers (i.e. contractors) who are contracted by DkIT to provide goods and services (for example: technical support, consultancy etc.).

Remote access services for staff, students, guests or contractors must be reviewed and approved by the IT Manager in conjunction with department heads (refer to the user administration documentation).

This is to ensure that the user meets the appropriate criteria (as above): Staff, students, guests or contractors.

Staff must only be granted access to network facilities, services and information systems which are necessary for the employee to carry out the responsibilities of their role or function.

Contractors access requests must be sponsored by the specific Department / service owner (or nominee) engaging the service provider.

Remote user's access rights and privileges will be restricted to the minimum services and functions as is necessary for them to carry out their role from a remote site.

The Computer Services Department reserves the right to block a remote access request on technical, operational or security grounds.

All confidential and restricted information transmitted via a remote access connection must be encrypted prior to transmission or sent through an encrypted tunnel e.g. Citrix. Secure web access is via https://remote.dkit.ie. Secure data delivery can be over https://filesender.heanet.ie

Remote access connections must only be used for approved DkIT business/academic purposes.

Remote Access Approvals

Staff

Staff have remote access to web and desktop services by default. A standard desktop service is made available to all staff users to allow access to the user's personal home directory. A standard suite of packages (Microsoft Office) are available to the user to operate on home directory data. The desktop service also provides access to specific packages e.g. Core/ESS. For other applications the line manager must request access to specific applications that the user requires.

Students

Students have access to web services as part of the education programme delivery. Secure access is available based on user authentication against Active Directory services, Web services such as email & Moodle i.e. services that provide access to course content is based on user's registration status and specific course details.

Desktop services are not provided to Students (November 2018). Access rights will be based on student registration status and access to applications will be based on the academic department that the student belongs to.

Staff and Student users are auto provisioned.

- Students are provisioned by Banner System
- Staff members are provisioned based on details entered on CoreHR Personnel system.

As per GDPR requirements staff and student systems are reviewed on a bi-annual basis to establish user account access rights.

Contractors

Contractors i.e. Third-party commercial service provider may need to have access to specific systems and services on the network as opposed to specific applications.

Such requests must be sponsored by the specific department / service owner (or nominee) engaging the service provider with final approval by the IT Manager. There is a specific policy relating to Third Party / Contractor Access "Outsourcing_3rd Party Access Policy.docx".

Access to Services

A contractor will only be granted remote access to the DkIT network and information systems after the computer services department has received the appropriate notification / documentation in respect of authorised personnel who will be supporting DkIT systems.

A Contractor remote access account will be created and reviewed every 6 months and will be monitored in accordance with the user administration procedures / Access Control Policy

Implementing Remote Access Policy

Remote Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant DkIT policies, procedures, regulations and applicable legislation;
- Ensuring they only use remote access accounts and passwords which have been assigned to them;
- Ensuring all remote access account passwords assigned to them are kept confidential at all times and not shared with others;
- Changing their passwords in compliance with the password standard or when instructed to do so by designated system administrators, network administrators or the Computer Services department;
- Respecting and protecting the privacy and confidentiality of the information they process at all times;
- Ensuring they use their remote access connection in a lawful and ethical manner at all times;
- Complying with instructions issued by the Computer Services department on behalf of DkIT;
- Reporting all misuse and breaches of this policy to their line manager.

Compliance

DkIT reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. DkIT staff, students, or contractor who breach this policy may be subject to a disciplinary action.

Breaches of this policy by a contractor, may lead to the withdrawal of DkIT information technology resources to that third party and/or the cancellation of any contract(s) between DkIT and the contractors i.e. the service provider.

Review & Update

This policy will be reviewed and updated on a period basic to ensure that any changes to the DkIT's organisation structure and business practices are properly reflected in the policy.

Related Documents / Policies:

- Logical Access Policy
- Physical Access Policy
- Outsourcing_3rd Party Access Policy
- User Administration Procedure