Dundalk Institute of Technology

Anti-Virus Scanning and Protection Standard

Version 1.3

Document Location

..\DkIT_Policy_Documents\Standards and Guidelines

Revision History

Date of this revision:	Date of next review:

Revision Number	Revision Date	Summary of Changes	Changes marked
1.0	15/5/15	Review of AV Scanning & Protection Document	
1.1	18/11/15	Review of Document prior to approval	
1.2	06/07/18	Revised Roles and responsibilities	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
V1.2	07/09/18	James McCahill Loretto Gaughran	Review document for General Data Protection Regulation - compliance
V1.3	24/09/18	James McCahill Michael Denihan	Review document for approval

Approval

This document requires the following approvals:

Name	Title	Date
James McCahill	IT Manager	24/09/18
Michael Denihan	Computer Services Manager	24/09/18

It 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 ensuring that the IT resources and services it delivers operate on secure pc and server equipment. To this end an anti-virus policy has been developed for guidance to ensure a secure operational environment for the IT services platform and users.

2 Purpose

The purpose of this Anti-Virus and Protection Standard is to provide specific guidance to Dundalk Institute of Technology staff in relation to anti-virus controls. This standard should be read in conjunction with Dundalk Institute of Technology Information Security Policy.

3 Definitions

Antivirus or anti-virus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware, adware and malware in general.

Virus

A computer virus is a computer program that can copy itself and infect a computer. The term "virus" is also commonly referred to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability. A virus can spread from one computer to another when its host is taken to the target computer; for instance, if a user sent it over a network or the Internet or carried it on a removable medium such as a DVD or USB key. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Trojan Horses

A trojan horse, or trojan, is software that appears to perform a desirable function for the user prior to run or install, but (perhaps in addition to the expected function) steals information or harms the system.

Malware

Malware (malicious software) is software designed to harm or secretly access a computer system without the owner's informed consent.

Adware

Adware (advertising-supported software) is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up.

Spyware

Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

4 Roles and Responsibilities

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

Senior Leadership Team	The Senior Leadership Team is responsible for the internal controls of Dundalk Institute of Technology, The SLT is responsible for: • Reviewing and approving this Standard and any updates to it as recommended. • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility. • Ensuring oversight of appropriate IT Usage or either through their own work or other governance arrangement. • To ensure the Policy is reviewed and approved by the Governing Body. • To liaise with appropriate staff 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.
Staff	To ensure that they follow the Anti-Virus and Protection Standard when using Dundalk Institute of Technology IT Resources and accessing Dundalk Institute of Technology Information assets to carry out their job functions or complete their programme of study. Also ensure that Staff have taken appropriate security precautions on their own equipment whilst connecting to the Dundalk IT network infrastructure. To inform IT Staff on any issues on virus detection.
Students	To inform Staff of any breaches / noncompliance of this standard on DkIT equipment that they are using To ensure that Students have taken appropriate security precautions on their own equipment whilst connecting to the Dundalk IT network infrastructure.
IT Manager	To monitor compliance with the Anti-Virus and Protection standard. To inform the Vice President for Financial and Corporate Affairs of suspected non-compliance and/or suspected breaches of the Anti-Virus and Protection standard.

5 Scope

This document outlines the general guidelines to be followed by Dundalk Institute of Technology staff in terms of anti-virus protection.

6 Anti-Virus scanning and protection standard

All devices that connect to the Dundalk Institute of Technology network must employ anti-virus software. All Dundalk Institute of Technology computer resources must run the Institutes anti-virus solution. Dundalk Institute of Technology reserves the right to disconnect any machine, device or resource that is deemed not to have adequate levels of anti-virus protection.

Dundalk Institute of Technology users are requested to:

- Always run the current version of the Dundalk Institute of Technology standard, supported anti-virus software.
- Update anti-virus software daily.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is a business requirement to do so.
- Always scan portable media from an unknown source for viruses before using it.

<u>Please note the following:</u>

- All DkIT owned devices connected to Dundalk Institute of Technology network are updated automatically
- All PCs/Laptops that have the antivirus software installed scan automatically.
- All PCs/Laptops in AD will have the software remotely installed on them by SCCM.
- PCs/Laptops not in AD will have to have the software manually installed by a technician. Please contact the Helpdesk.
- All electronic mail coming into or leaving Dundalk Institute of Technology is scanned for viruses.
- Viruses and Spam can be distributed to other users using web links that are emailed as part of a spam campaign. You should never respond to emails requesting user / password details to “confirm” user account details.
- BYOD must have up to date anti-virus software installed and kept current.

../