Title	**Anti-Virus and Malware Protection Policy**
Date	17th February, 2020
Approved By	LWETB Meeting 17th February, 2020
For Review By	LWETB Board

LWETB
Anti-Virus and Malware Protection Policy

1. Purpose

The purpose of the Anti-Virus and Malware Protection Policy is to establish principles which must be met to prevent viruses and malware from entering the LWETB's environment, to identify and report on malware or suspected malware attacks, and to define appropriate actions to eliminate and recover from malware related incidents.

Please note if there is anything in this Policy which is unclear or if you have any questions please contact ICT Support who will provide assistance.

2. Description

This policy applies to all LWETB employees and contractors using LWETB resources. It is the personal responsibility of each individual to take precautions to ensure that no form of virus or malware is introduced into any of LWETB's resources or systems with which they come into contact.

3. Definitions

For the purposes of this policy, we apply the term "Malware" to define all types of malicious software that performs malicious tasks like deleting files, changing computer settings, collecting personal information, gaining access to systems, holding the user to ransom etc. This includes Viruses, Worms, Trojans, rootkits, keyloggers, spyware, adware etc.

"Must", or the terms "required" or "shall", refer to an absolute requirement of the policy. "Must not", or the phrase "shall not", refer to statements which are an absolute prohibition of the policy. "Should", or the adjective "recommended" refers to a statement that should be applied. In certain circumstances, there may exist a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.
"Should not", or the phrase "not recommended" mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

All users must note and report any observed malware or suspected security incidents as soon as possible. Particularly virus outbreaks must be reported to LWETB ICT Support and to your Manager. All end-user devices connecting to LWETB resources must have appropriate anti-virus and malware protection installed and active. To protect against malware infections, an 'in-depth defence' strategy is required to minimise the risk of loss or damage to services.
This includes anti-malware security controls at: Client Level, Server Level and Network Perimeter.

4.1 Client Protection

All PCs and laptop equipment must have anti-virus software installed and active.

- All PCs and laptop equipment must have on-line (real-time) scanning enabled and enforced as a background service (i.e. each file access must be checked while loading).
- All PCs and laptop equipment should have a scheduled weekly scan at a minimum of all files for malicious code.

All PCs and laptops must have automated update mechanisms enabled and active to ensure they are provisioned with the latest virus signature files

4.2 Server Protection

All Microsoft based Servers must have anti-virus software installed and active. This includes:

- Real-time “on-access” scanning.
- Scheduled weekly scan for malicious code.

All anti-virus software must be configured to be updated automatically. The Virus Signatures should be updated (at a minimum):

- Daily for servers with network access to virus signature update server
- Weekly for other non-network connected servers

Servers with operating systems other than MS-Windows or UNIX are currently out of scope of this policy (e.g. Tru64/OpenVMS etc). In case such systems must be used, a case-based consultancy and evaluation must be carried out.

4.3 Network Perimeter Protection

Approved anti-malware solutions must be deployed at all internet and e-mail gateways to prevent malware from entering the network.
Email checking for malware must be performed at the e-mail gateway for both incoming and outgoing messages.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisational Support & Development	Revisions and updates to the policy
LWETB Management Team	Approval of the Policy
All End-users (refer to end-user policies)	Responsible for implementation of the policy.
Internal and external audit	Monitoring and reporting compliance with the policy
LWETB ICT Support	Tracking of calls related to Security Incidents