Policy Domain	**Antivirus Management Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Document Control			
Prepared By **Vineet Kumar Chawla** **(Sr. Consultant IT)**	**Reviewed By** **Maruti Divekar** **(IT Head)**	**Checked By** **B P Rauka** **(CFO)**	**Approved By** **Mukund Kabra** **(Director)**

Document Modification History

SR #	Document	Version No.	Reviewed On	Checked On	Approved On	Effective Date	Authorized Signatory
1.	Antivirus Management Policy	1.0	05TH Mar 21	10th Mar 21	10th Mar 21	11th Mar 21	
2.							
3.							

Document Control

- This document is subject to version control and shall be managed by IT Head. Any request for amending this document shall be approved by Director. The IT Head shall review this document at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes.

- The document is available on Helpdesk Portal under Announcement and Server shared folder under AETL Policies and provided with HR Joining Kit, in non-editable pdf format and all the employees are expected to read and adhere to it. The approved and signed copies are available with IT Team, which can be used for audit purpose only. IT Team is responsible for maintaining updated copy of this document and its effective communication within Advanced Enzymes (AETL).

Policy Domain	Antivirus Management Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

Policy Domain	Antivirus Management Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

1. Overview

Computer devices are any type of device connected to a network that could become infected with a computer virus. Examples of computer devices would be, but not limited to, workstations, servers, laptops, etc.

Malicious software is any type of computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, trojans, etc.

Anti-Virus software runs on either a server or workstation and monitors network connections looking for malicious activity or viruses.

This document describes the measures taken by the IT and end users to counter computer viruses and identifies the responsibilities of individuals, departments and IT Services in protecting the organization against viruses and other vulnerabilities.

2. Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers providing services or working at AETL, including all personnel affiliated with third parties. This policy applies to all equipment's that are owned or leased by AETL.

3. Purpose

The purpose of this policy is to help prevent infection of AETL computers, networks, and technology systems by computer viruses, malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files and hardware.

This document establishes the corporate policy and standards for anti-virus/malware protection on any system owned by AETL or connected to the AETL network. This policy will help ensure that all vulnerable computing platforms are guarded against vulnerabilities and protected by antivirus software at all times.

4. Ownership

The IT Head is the owner of this policy and System Administrator is responsible for maintaining it.

5. Policy

AETL shall adopt certain practices to prevent malware/Virus attacks or problems:

a) All workstations connected to AETL network must use AETL-approved anti-virus and anti-malware software and configuration.

b) Anti-virus software must be actively running on all devices that are connected to the AETL network at all times.
c) The anti-virus and anti-malware software must not be disabled or bypassed.
d) The settings for the anti-virus and anti-malware software must not be altered in a manner that will reduce the effectiveness of the software.
e) The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.
f) Every virus/malware that is not automatically cleaned by the anti-virus and anti-malware software constitutes a security incident and must be reported to the IT Helpdesk.
g) All workstations will be updated automatically by the central virus software installation servers where possible, if this is not possible then users will be shown how to update their virus software with the minimum of intervention of their part.
h) The Antivirus software is designed to start-up automatically when the PC starts up; this is to ensure that the PC is protected at all times.
i) When users receive a virus notification on their workstation, they are required to notify IT Helpdesk immediately.
j) An infected computer device will be disconnected from the AETL network until the infection has been removed or the system has been re-installed.
k) Users are prohibited from disabling, modifying or removing AETL provided anti-virus software.
l) All removable media that will be used on PCs must first be virus scanned to ensure that there are no viruses resident on the media.

Virus detection (or suspected infection)

In the event that a virus is found or suspect on a user's PC, they should contact the IT Helpdesk immediately. The user must follow the instruction of the IT staff, which may involve ceasing all work on the PC and labelling it so that other people do not attempt to use it.

If the PC is connected to the Network (or via Wifi / Data Card) they must disconnect immediately, i.e. if connected to the Network remove Network cable from the wall or if using WIfi / data card disconnect the same.

The IT department will investigate the incident and will undertake any remedial work to resolve the issue.

6. Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any.

IT Head will be responsible for reviewing the policy and communicating the changes made therein.

7. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Domain	**Antivirus Management Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

8. Roles & Responsibility Matrix (RACI)

Activity \ Role	IT Head	ISMS Steering Committee	Internal Users	External Users	Exempted
Authoring of this document	RA	RA	-	-	-
Approval of this document	I	CI	-	-	-
Sign-off of this document	CI	CI	-	-	-
Application of this document	RA	RA	RA	RA	-

R	Responsible
A	Accountable
C	Consulted
I	Informed

9. ISMS Steering Committee Members

1. Mukund Kabra (Director)
2. B. P. Rauka (CFO)
3. Maruti Divekar (IT Head)

10. AETL IT Helpdesk Contact Details

- Logging an online support request: **https://192.168.2.7:8080**
- Email: **it.helpdesk@advancedenzymes.com**
- Telephone: **022 41703234**