ANTIVIRUS POLICY

**REVISION HISTORY:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Doc.No** | **Prepared By** | **Approved By** | **Release Date** | **Changes Made** |
| KAL\_Antivirus Policy\_01 | Mrs. Poongodi Guruvareddy | Mr. Kubendran | 25/Jan/2021 |  |
| KAL\_Antivirus Policy\_V1.1 | Mrs. Aishwarya | Mr. Kubendran | 27/Sep/2022 | Classification of document done |
| KAL\_Antivirus Policy\_V1.2 | Mr.Raja Sarath | Mr. Kubendran | 09/Sep/2024 | Classification of document done |
|  |  |  |  |  |

Table of Contents:

[Overview of the Document 4](#_Toc322422113)

[1. Purpose 4](#_Toc1699289509)

[2. Scope 4](#_Toc116350565)

[3. Policy 4](#_Toc1107640918)

[4. Policy Compliance 4](#_Toc1598180093)

[5.1 Compliance Measurement: - 4](#_Toc1479034707)

[5.2 Exceptions 5](#_Toc1897966515)

[5.3 Non-Compliance 5](#_Toc865983409)

[5. Appendix: 5](#_Toc877213484)

[Guidelines on Antivirus 6](#_Toc883299180)

# Overview of the Document

See Purpose

# **Purpose**

To establish requirements which must be met by all computers/ Laptops connected to Kalpita Technologies networks to ensure effective virus and other malware detection and prevention.

# Scope

This policy applies to all Kalpita Technologies computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based equipment such as traffic generators.

# Policy

All Kalpita Technologies PC-based computers/Laptops must have Kalpita Technologies standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Admins/ Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Kalpita Technologies networks (e.g., viruses, worms, Ransom ware, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Monitoring of the anti-virus installations and taking periodic reports (monthly) review and approve & maintain it.

**Symptoms of an Infected computer: –**

* Computer fails to start
* Programs will not launch, or they fail when simple commands are performed
* Names of files are changing or become unreadable
* File contents change or are no longer accessible
* Unusual words or graphics appear on the screen
* Hard or floppy disks are formatted
* Variations occur in computer performance, such as slowing down in loading or operation.

*[****Refer to Kalpita Technologies Anti-Virus Recommended guidelines under Appendix section to***

***help prevent virus problems*.**]

|  |
| --- |
| **Noted exceptions:** Machines with operating systems other than those based on Microsoft products  are excepted at the current time. |

# Policy Compliance

## 5.1 Compliance Measurement: -

The IT team will verify compliance with this policy through various methods, including periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## 5.2 Exceptions

Any exception to the policy must be approved by the IT team in advance.

## 5.3 Non-Compliance

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

# Appendix:

## **Guidelines on Antivirus**

**Recommended processes to prevent virus problems:**

* Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
* NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
* Delete spam, chain, and other junk email without forwarding, in with Kalpita technologies’ Acceptable Use Policy.
* Never download files from unknown or suspicious sources.
* Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
* Always scan a floppy diskette from an unknown source for viruses before using it.
* Back-up critical data and system configurations regularly and store the data in a safe place.
* Unneeded services should be turned off and removed.
* 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 Team.
* Anti-virus logs should be maintained for 21-30 days (about 4 and a half weeks).
* IT Team to review the above-mentioned logs and identify any threats/vulnerabilities
* The anti-virus and anti-malware software must not be disabled or bypassed.
* The settings for the anti-virus and anti-malware software must not be altered to reduce its effectiveness.
* The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.
* Always keep patch level up-to-date, especially on computers that host public services and are accessible through the firewall. such as HTTP, FTP, mail and DNS services.

**Disclaimer**:

These policies and disclaimers are provided for informational purposes only and are not meant to be a contract of any type. Benefits may change sometimes. Company reserves the right to change or discontinue these policies, procedures, and benefits in its sole discretion.