**Virus Management Policy And Procedure**

Doc:/POL/0.1

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Virus Management Policy and Procedure |
| --- | --- |
| Document ID | /POL/0.1 |
| Security Classification | Internal |

| **Authorization** | | |
| --- | --- | --- |
| Document Owner | Reviewed by | Authorized by |
|  |  |  |

| **Amendment Log** | | | |
| --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Section** | **Brief description of the change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

1.0 Purpose 4

2.0 Scope 4

3.0 Responsibility 4

4.0 Policy and Procedure 4

4.1 Virus Protection and Prevention 4

4.2 Virus Reporting 5

4.3 Installation of Anti-Virus Software 5

4.4 Updating Anti-Virus “Virus Definition Files” 5

4.5 Anti-Virus Software Upgrades 5

4.6 Periodic Review 5

5.0 Reference Documents 6

# Purpose

To detect, contain and correct incidents of computer viruses, worms, and Trojan horses. Anti-virus software shall be installed and regularly updated on all systems in the network. All systems shall be scanned for virus attacks regularly.

# Scope

The policy outlined in this document applies to all employees and all information resources as well as the application and systems software.

# Responsibility

The Head – IT is responsible for ensuring the implementation and execution of the procedures mentioned in this document. The Management Representative shall periodically review and monitor the virus management procedure to ensure adherence to the procedures in this document.

The Head - IT shall appoint a designated coordinator for antivirus management.

# Policy and Procedure

* The viruses and malicious software are unauthorized programs that replicate themselves and spread to other computer systems across a network. The symptoms of Virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.
* Upon encountering the virus attack, the user must immediately stop using the affected computer and report it to the IT Helpdesk. As the viruses have grown very complex, users must not attempt to eradicate them without expert advice.
* The eradication of virus problems by IT engineers alone would ensure that infections are centrally reported. The virus logs utility in Antivirus (AV) software is enabled and the logs are reviewed daily by the IT engineer responsible for the AV software and periodically by the Manager - IT. Upon encountering the virus, the IT engineer on shift immediately handles the situation.
* The IT Team shall ensure that AV software is installed on all systems. IT Team shall ensure that they are installed with the latest version of AV software. The “Virus Definition Files” of AV software shall be updated via LIVE update.
* The upgrades are the newer versions of the AV software. The IT Team is responsible for AV software upgrades and will procure newer versions/engines of AV programs. Any new upgrades once approved by the Head - of IT, the IT Team shall ensure a quick rollout of the same across the organization.
* The IT team shall verify the following:
  + Ensure that the AV software is installed on every machine.
  + The AV software is scheduled to run daily.
  + Ensure the software is working optimally. Upon encountering the virus problem, the AV software stops operations of the affected gadget, quarantines and deletes the related files, and cleans the affected areas. The other options such as “continue” and “move to a directory” in AV check are not enabled.

## Virus Protection and Prevention

* Every user should ensure the presence of the anti-virus agent on their desktops and report immediately to the IT department if not present.
* Rampant usage of external media such as but not limited to pen drives, and USB devices is prohibited.
* Employees shall not change the anti-virus settings and configurations.
* Due care shall be taken to update laptops with latest copy of anti-virus signatures as they are mobile and not easily accessible.
* Any type of suspicious virus-like activities should be immediately brought to the notice of the IT Team. A few examples of suspicious activities, however not limited to, are mentioned below:
  + Unusual email messages, pranks, display.
  + Significant extension of time to access disks.
  + Unusual disk space and/or memory usage.
  + Tampering or change in file contents, size of the file, date, and time stamp.
  + Abnormal application behavior or low response time.
  + Any other unnatural, irregular, or exceptional activity.

## Virus Reporting

Upon encountering the virus attack, the user must immediately stop using the affected computer and report it to the IT Helpdesk. As the viruses have grown very complex, users must not attempt to eradicate them without expert advice.

The eradication of virus problems by IT engineers alone would ensure that infections are centrally reported. The virus logs utility in antivirus (AV) software is enabled and the logs are reviewed daily by the IT engineer responsible for the AV software and periodically by the Manager – IT. Upon encountering the virus, the IT engineer on shift immediately handles the situation and raises a security incident.

## Installation of Anti-Virus Software

Head – IT shall ensure that the latest version of AV software is installed on all systems within the network. Virus control at the gateway and email level is also managed by the IT Team.

## Updating Anti-Virus “Virus Definition Files”

The “Virus Definition Files” of anti-virus software shall be updated as follows:

Automatic Update:

* A console server will be configured to check the parent site at a scheduled time for any new virus updates.
* If there is any update it will be downloaded and from the server, it will be scheduled for pushing these Virus Definition Files onto servers/client computers/laptop computers/network nodes connected.
* This job shall be scheduled to run immediately after copying the Virus Definition Files on the -central host computers or during the next user logon.

## Anti-Virus Software Upgrades

The upgrades are the newer versions of the anti-virus software. Head – IT shall scan for upgrades and decide to procure newer versions/engines of AV programs, as needed. Any new upgrades shall be approved by the Head – IT and Manager – IT will ensure a quick rollout of the same across the organization.

## Periodic Review

IT Team shall verify the following:

* Ensure that the AV software is installed on every machine.
* The AV software is scheduled to run as configured. However, it may be noted that since the file system, auto-protect option / real-time protection is enabled on all antivirus installations, the daily scheduled scan is an optional component.
* Review the anti-virus software activity/logs to check whether the AV system is running regularly on desktop computers.
* Ensure that the AV software is working optimally. Upon encountering the virus problem, the AV software stops the operations of the affected gadget. For severe and high alerts, the AV software deletes the related files and cleans the affected areas. For medium alert, the AV software quarantines the files.
* The AV software for the messaging system (e-mail) has also been centrally implemented. If the virus is found in the mail attachment file, the AV software pops up the virus detected message on the client’s system as well as the System Centre Console.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of Applicability for ISO 27001:2013
* IT Tickets (Service Desk) for virus reporting