

Document Name	CSE Anti-Virus Policy
Document Creation Date	31/03/2003
Document Created By	GM-ITD
Version Control History	1.5
Document Reviewed Date	05/12/2024
Document Reviewed By	CISO-CSE
Document Approved By	Standing Committee on Technology

CSE Anti-Virus Policy

1.0 Purpose

To establish requirements which must be met by all computers connected to The Calcutta Stock Exchange Ltd. (CSE) screen based trading and other computing infrastructure including hardware and networks to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all CSE and its subsidiary CCMPL computers that are Windows-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, other servers, and any other PC based equipment including attendance recorder.

3.0 Policy

All CSE and CCMPL Windows-based computers must have CSE's 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.

Officer in charge of each department is responsible for ensuring that anti-virus software is kept up-to-date and run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into CSE's networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

4.0 Procedure

Prevention and cure procedures for virus related problems are given in CSE's *Anti-Virus Recommended Processes*.

5.0 Enforcement

Any Exchange employee, or employee of a vendor of the Exchange or any member including their employees/assignees or vendors personnel working on behalf of the member found to have violated this policy may subject the responsible entity to disciplinary action.

6.0 Exceptions

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

CSE Anti-Virus Recommended Process

Recommended processes to prevent virus problems:

- Antivirus software should be implemented at various levels (e.g.: Desktop, Laptops, Email Gateways & Web Gateway in the Perimeter network) in the network and system infrastructure, as applicable, as part of a layered approach to minimizing malicious code entry in to CSE Computing environment.
- E-mail attachment types such as but not limited to “.exe, .bat, cmd, .scr, .pif” through emails should ideally be blocked at the Email gateway level for preventing malicious code intrusion into CSE Network and for hosted mail service users, the above types attachments ideally to be avoided or thoroughly virus checked and then accessed if at all necessary.
- Users should immediately disconnect his/her desktop/laptop from the network in case of suspicious presence of malicious code/virus (if any) and report it to the concerned Departmental Head/Officer-In-Charge as soon as these are noticed.
- Users should report any abnormal behaviour in Computer System such as slow processing of applications, continuous/ prolonged hard disk /network activity etc., to the concerned Departmental Head/Officer-In-Charge for appropriate action.
- System Administrator / Data Centre Team of CSE should be responsible to ensure virus free release of all new software.
- System Administrator / Operations Team should certify and ensure provisioning of virus free IT resources, during new implementation of hardware, OS implementation and storage media replacements.
- Users should install & use only licensed software on CSE computing resources and are responsible for availability/detection or usage of any unlicensed software on their desktops/laptops.
- Always run the CSE standard, supported anti-virus software, which is available in the Information Technology Division section of CSE website. Install/apply 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.
- Never copy/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.
- Avoid using and inserting USB pen drive. If unavoidable circumstances always scan a USB device from an unknown source for viruses before using it.

- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- New viruses are discovered almost every day. Periodically check the *CSE Anti-Virus Policy* and this Recommended Processes list for updates.

Centralized Anti-Virus Management

- Preferably a full scan should be scheduled for all workstations and servers connected to the Central Virus Control Unit on daily basis in non-peak hours.
- Antivirus software must be monitored regularly so that any virus incident can be quickly dealt with.
- Should provide real-time status of the all connected PCs & Servers to enable the administrator immediately detect any virus incident occurred.
- Special attention must be paid to ensure that antivirus scanning programs are using the most current pattern file, scan engine and program version.
- It is recommended to maintain Anti-virus logs for a period of 7-15 days or as determined by the Organization. Ideally, a weekly analysis of the logs should be done to obtain an infection profile of viruses and the machines infected.

CSE Antivirus Updation Procedure

In phases, the Exchange has procured various anti-virus software which are deployed in different application areas. This document aims to bring about a comprehensive procedure for upkeep of these with latest downloads of virus definition.

- Following a predefined schedule, (preferably on a designated day of each week), the latest virus definition file for each of the products in use in the Exchange will be downloaded by designated CSE official. All such definition files would be handed over to the operations group who would then make these files available for download through the CSE network.
- All departmental heads/officer-in-charge for specified functional area would ensure that all the computers used in the department/functional area is updated with the latest definition files periodically.
- However, each user is individually responsible for keeping his/her computer free from virus.

Detailed procedure for Distribution of Latest Antivirus software

The relevant computers of Calcutta Stock Exchange Associations are protected by antivirus software like Kaspersky. PCs with internet would automatically download patches from antivirus provider's site automatically. Now as the central virus control unit is in place the antivirus definition and updates would be downloaded daily on that central antivirus server and automatically deployed to the connected client PCs. Those who are not connected to the server (not in LAN) would either download the update patches daily from internet or update patches will be installed by the support engineers weekly.

Following routine jobs will be done by all computer users of the exchange to protect computers from virus attack:-

- Every day quick scanning and repairing of all relevant fixed drives for computer virus infection.
- User's PCs are restricted from any downloads from the internet for security reason
- Be sure that online monitor for anti virus is on for all incoming and outgoing files.

Version Control History

Version Change Date: 02/11/2022

Version Number: 1.4

Changes:

- Acceptable Use Policy has been developed
- First 7 points under 'Recommended processes to prevent virus problems' has been added
- A new section Centralized Anti-Virus Management has been added with all its processes

Version Change Date: 05/12/2024

Version Number: 1.5

Changes:

- Use of McAfee Anti-Virus software and its updation process in Section-13 Servers has been deleted as Section-13 arrangement has been stopped since November 2023.