CHENNAI PORT TRUST

Anti-Virus Policy

Purpose

One of the goals of Chennai Port Trust is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Chennai Port employees to help achieve effective virus detection and prevention.

Definition

Virus

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, thumb drives, and CDs etc. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user.

Scope

This policy applies to;

1. All employees using Chennai Port computers connected to the network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the company's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

2. Other persons working for Chennai Port Trust, such as, persons engaged in business transactions or contractors, using any computer and network of Chennai Port Trust.

General Policy

1. Chennai Port Trust was using Symantec End point anti-virus protection, Currently, Chennai Port Trust has Kaspersky Anti virus solution (Version: Total Security:2017) installed. The most current available version of the anti-virus software package will be taken as the default standard.

2. All computers attached to the Chennai Port Trust network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the Chenai Port Trust network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT(EDP) department immediately, Ext. 2462. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.

6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by Chennai Port Trust.

2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Files with the following filename extensions are blocked by the e-mail system: [.exe, .bat etc.]. Business files with banned extensions can be sent/received by compressing the same in a folder by use of a file compression utility.

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7. Avoid direct disk sharing with read/write access. Always scan any storage media for viruses before using it.

8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

CHENNAI PORT TRUST

IT Department Responsibilities

The following activities are the responsibility of the Chennai Port Trust IT department:

1. The IT department is responsible for maintaining and updating this Anti-Virus Policy.

2. The IT department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

3. The IT department will apply any updates to the services it provides that are required to defend against threats from viruses.

4. The IT department will install anti-virus software on all Chennai Port Trust owned and installed desktop workstations, laptops, and servers.

5. The IT department will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IT department will provide anti-virus software in these cases.

6. The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

7. The IT department will perform regular anti-virus sweeps of Windows desktop OS and user files.

8. The IT department will attempt to notify users of Chennai Port Trust systems of any credible virus threats via IP messenger. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

Department and Individual Responsibilities

The following activities are the responsibility of Chennai Port Trust departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.

2. All employees are responsible for taking reasonable measures to protect against virus infection.

3. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Chennai Port Trust network without the express consent of the IT department.