Anti-Virus Policy

Purpose

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, flash disks and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to USEK in terms of lost data, lost staff productivity, and/or lost reputation.
As a result, one of USEK's goals 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 USEK employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the USEK network via a standard network connection, wireless connection or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the USEK network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

General Policy

1. Currently, USEK has a Business edition of Antivirus and Antispyware software. Licensed copies of ESET NOD32 Antivirus 5 can be obtained at http://www.eset.com. The most current available version of the anti-virus software package will be taken as the default standard.

2. All computers attached to the USEK 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 USEK 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 department immediately at Service Desk Support - 1414. 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 USEK.

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 co-worker) 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 mail filter system:".exe".

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

7. Avoid direct disk sharing with read/write access. Always scan any disk 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.

IT Department Responsibilities

The following activities are the responsibility of the USEK IT department:

1. The IT department is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted at the IT department archive. Check one of these locations regularly for updated information.

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. An automatic update is performed three times per day.

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 USEK 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 ESET Nod 32 files.

8. The IT department will attempt to notify USEK users of any credible virus threats via e-mail or telephone messages. 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 USEK 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. Departments, that allow employees to use personally-owned computers for business purposes, must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

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

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

Enforcement

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

Declaration of Understanding

I, [employee name], have read, understand, and agree to adhere to USEK's Anti-Virus Policy.

Name (Printed): _____

Name (Signed): _____

Today's Date: _____