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 email or instant messaging attachments, downloadable Internet files, diskettes, 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 Cornwall-Lebanon School District in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Cornwall-Lebanon School District 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 Cornwall-Lebanon School District employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the Cornwall-Lebanon School District network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both district-owned computers and personally-owned computers attached to the Cornwall-Lebanon School District's network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

Policy Statements

1. Currently, Cornwall-Lebanon School District has Microsoft ForeFront Antivirus. The most current available version of the anti-virus software package will automatically be pushed to all district owned machines.

2. All computers attached to the Cornwall-Lebanon School District's network must have standard, supported anti-virus software installed. This software must be active, 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 Cornwall-Lebanon School District network (e.g. viruses, worms, Trojan horses, email 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. 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.

Relevant Procedures

1. Always run the standard anti-virus software provided by Cornwall-Lebanon School District.

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

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

4. Be suspicious of email messages containing links to unknown websites. 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. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

6. Avoid direct portable drive (e.g. memory stick) sharing with read/write access. Always scan a portable drive for viruses before using it.

7. If instructed to delete email messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

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

9. 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.

The following activities are the responsibility of Cornwall-Lebanon School District 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 Cornwall-Lebanon School District network without the express consent of the IT department.

Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at Cornwall-Lebanon School District. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable Cornwall-Lebanon School District policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.