Overview

All Windows and Macintosh computers (clients and servers) connected to the Central Dauphin School District computer or networked resources shall have supported antivirus software (preferably the most current version) correctly installed, configured, activated and updated with the latest version of virus definitions before or immediately upon connecting to the network. If deemed necessary to prevent viral propagation to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code (herein collectively referred to as “malware”) shall be disconnected from the network until the infection has been removed.

When an enterprise-wide virus attack is in progress, ITCS shall notify the campus computing community via the best available method, and all files on all hard drives should be scanned immediately using the newest virus definitions available.

Other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

Any exceptions to this regulation must be explicitly approved by the IT Director.

Areas of responsibility

Information Technology Services department Staff

All Employees, students and personnel

Procedure details

All Pcs, Laptops, and Servers must have the latest Antivirus program and latest virus definitions installed before they can operate on the district network.

The Client Services division of the Information Technology Services department is responsible and will install and configure the latest Antivirus program and latest virus definitions on all Pcs and Laptops and before deploying any new equipment, image or virtual machines (VMs) into production.

The Network Service division of the Information Technology Services department is responsible and will install and configure the latest Antivirus program and latest virus definitions on all Servers and before deploying any new equipment or virtual machines (VMs) into production.

The Network Services division of the Information Technology Services department will monitor equipment in real time via the enterprise console. Minor issues such as out of date computers or anti-virus policy errors will be address and attempted to be resolved during the Weekly checks. Each major threat will be addressed immediately and cleaned. If a
piece of equipment cannot be cleaned, it will be removed from the network immediately. If a virus is found or suspected users should shut down their computer and call the District helpdesk at (717) 346-9452 or 70452 from any district phone.

References

http://www.sophos.com

Help page

http://cdnet