Anti-Virus Procedure

Procedure Number: PSU-NK-ITS-006
Date: September 28, 2017
Page Count: 3

Purpose:

This procedure will provide best practices and guidelines as it pertains to the installation and continued support of anti-virus software installed on all devices connected to the Penn State New Kensington Data Network to ensure effective virus detection and prevention exists on all systems.

Scope:

This procedure applies to all devices that connect to the Penn State New Kensington Data Network.

Definitions:

Device – A computer, electronic tool or communication apparatus with the ability to connect to a data or communication network.

New Kensington Data Network – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

NK ITS Department – The department that oversees IT resources at Penn State New Kensington to include the System Administrator, IT Specialist and IT Director

Procedure:

All devices connecting to the New Kensington Data Network that are capable of running a reputable anti-virus software, must have anti-virus software installed and scheduled to scan the system at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date.

Virus-infected devices must be removed from the network until they are verified as virus-free. The campus' system administrators are responsible for creating procedures that ensure anti-virus software is run at regular intervals for University owned devices, and devices are verified as virus-free.

Any activities with the intention to create and/or distribute malicious programs in or on the New Kensington Data Network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

PennState
New Kensington

University Owned Devices (Faculty, Staff, and Computer Labs)

- All University owned devices are required to have a managed anti-virus solution installed.
- Virus definition updates must be configured to install automatically.
- The anti-virus software configuration and status may only be changed by NK ITS Department personnel. Configuration changes by a system level user (limited user) are prohibited.
- Removing or disabling the anti-virus software by users other than approved NK ITS Department personnel is prohibited.

Non-University Owned Devices (Student and Visitors)

- All Non-University devices that connect to the New Kensington Data Network are required to have a reputable anti-virus solution installed.
- Virus definition updates must be configured to install automatically.

Recommended processes to prevent virus problems

- Download and run the current University site licensed anti-virus software, which is available from the http://downloads.its.psu.edu for free.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately. Empty the mail applications trash to be certain they are completely deleted.
- Use caution when opening links contained in emails. Move your mouse over the link and verify that the text for the link matches the URL for the website.
- Avoid suspicious websites.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is a significant business requirement to do so.
- Always scan any media (USB Flashdrives, Portable Hard Drive) 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 (See Data Backup and Retention Procedure).
- If anti-virus software conflicts with other software that is installed on the device, contact the Information Technology Service department for assistance.

Enforcement:

Devices found to be in violation of this procedure may be disconnected from the network until they are found to be in compliance or until a justifiable reason for not running current antivirus software is accepted.

Procedure History:

September 28, 2017 – Procedure created based off previous campus policy.