

ANTIVIRUS

POLICY NUMBER: IT-ANTIVIRUS

POLICY TYPE: ADMINISTRATIVE

RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT OF ADMINISTRATION & FINANCE

RESPONSIBLE OFFICE: CHIEF INFORMATION OFFICER

EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 6/07/2018

NEXT REVIEW DATE: PREVIOUS REVIEW PLUS FOUR (4) YEARS – 6/16/2026

SUPERSEDES POLICY DATED: 9/01/2009

BOARD OF REGENTS REPORTING (CHECK ONE):

PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM)

PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

In order to protect the campus computing infrastructure, Northern Kentucky University (NKU) requires the use of antivirus software on all computers that connect to the NKU network. This policy addresses the computer antivirus requirements for connection to NKU network(s) to ensure safe, secure, and effective virus detection and prevention.

- All computers and computing devices attempting to use the NKU network(s) must have antivirus software installed, kept up-to-date, and scheduled to run at regular intervals. For a list of some antivirus software, see the [antivirus section on the NKU Security website](#).
- The antivirus software must be kept up-to-date, per software vendor available updates, and must scan regularly.
- All Operating Systems (e.g., Windows, Mac, Linux) must be kept up-to-date with current patches per the Operating System provider.
- All NKU-managed and owned computers such as faculty, staff, and lab computers will have the university-owned and licensed antivirus tools installed and will be automatically scanned on a weekly basis.
- Non NKU-managed and owned computers such as students' computers or personal computers will be the responsibility of the owner to install and maintain the antivirus software, kept up-to-date, and scanned regularly, as stated above.
- Virus-infected computers will be removed from the network until verified as virus free. The user may incur charges if the computer requires service or virus removal efforts.

Note: Simply having an antivirus tool installed and scanning a computer does not guarantee that it will be safe from all viruses. Anyone suspecting a computer has been infected in any way and needing assistance should call the IT Help Desk at (859) 572-6911, or email itsecurity@nku.edu. New viruses are discovered frequently, so please check the IT Security website periodically for updates and new threats.

ENFORCEMENT

Any employee, student, or other user within the university network found to have violated this policy:

- May be removed from the network

- May be subject to disciplinary action, up to and including termination of employment or expulsion
- May be personally responsible for any fees, charges, or other costs to repair the computer and/or any damages to NKU network or infrastructure

Please see the [Acceptable Use policy](#) for additional details on IT usage and policy enforcement.

II. ENTITIES AFFECTED

This policy applies to all computers or devices that connect to or utilize the NKU network, file directories, or any network server interaction including, but not limited to, desktop computers, laptop computers, file servers, and mobile devices, regardless of ownership or administrative rights of the computer.

III. DEFINITIONS

NKU NETWORK

Being connected to a NKU network includes the following:

- Network capable devices (e.g., laptop) plugged into an NKU network port are connected to the NKU LAN (local area network).
- Wireless capable device (e.g., laptop, iPhone) connected to NKU Wireless SSID (e.g., NKU Public, Secure, or Encrypted) are connected to the NKU WLAN (wireless local area network).
- Connections from a computer through the NKU VPN (virtual private network) are connected to the NKU LAN (local area network).

IV. EXCEPTIONS

Exceptions are limited in regards to antivirus protection measures; therefore, they would only be considered on an extreme basis and may require approval by the area's vice president or Student Affairs management. Please contact itsecurity@nku.edu to address and review exception requests.

V. REFERENCES AND RELATED MATERIALS

RELATED POLICIES

[Acceptable Use policy](#)

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
Review and Minor Edits (wording, formatting, URLs)	June 16, 2022
Revision	June 7, 2018
New Policy	September 1, 2009

ANTIVIRUS

PRESIDENTIAL APPROVAL

PRESIDENT

Signature



Date 6/27/18

Gerard St. Amand

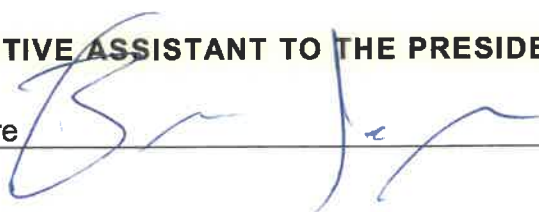
BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

- This policy was forwarded to the Board of Regents on the **Presidential Report (information only)**.
Date of Board of Regents meeting at which this policy was reported: 9 / 12 / 18.
- This policy was forwarded to the Board of Regents as a **Presidential Recommendation (consent agenda/voting item)**.
 - The Board of Regents approved this policy on ____/____/____.
(Attach a copy of Board of Regents meeting minutes showing approval of policy.)
 - The Board of Regents rejected this policy on ____/____/____.
(Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

EXECUTIVE ASSISTANT TO THE PRESIDENT/SECRETARY TO THE BOARD OF REGENTS

Signature



Date 9.18.18

Benjamin Jager