UNIVERSITY OF Cincinnati Clermont College	*Procedure/Guideline Title:* **Malware Protection**	*Number:* **034.TS.105**
Category: Information Technology **Applicable for:** Faculty/Staff/Students	**Effective Date:** 1.23.2023 **Prior Effective Date:** 11.16.2016 **Enabling Act:** Technology Steering Committee Approval	**Owner:** Technology Steering Committee **Responsible Office(s):** Technology Services

Background

As an institution of higher learning, UC Clermont both uses information technology and supplies it to the members of the university community. The guidelines contained in this document have been developed to create a framework to help ensure a safe and secure technology infrastructure for all faculty, staff, students and visitors at the college. The primary directive of technology at UC Clermont is to support, promote and enhance the learning process.

As per the University of Cincinnati's policy on Information Technology, all operating units that use information technology shall be responsible for:

- Developing and implementing, when appropriate, additional IT policies, guidelines or procedures specific to their academic or administrative units.

Guidelines

It is the responsibility of everyone who uses UC Clermont's computer network to take reasonable measures to protect that network from virus infections.

How do you get a virus?

Viruses can be received from downloading or receiving a file in the following ways:

- Receiving email with an attached file that contains a virus and opening or executing the file.
- Receiving email with a web link and opening or clicking the link.
- Downloading a file from the Internet that contains a virus and opening/executing the file.
- Transmitting by computer networks and/or by sharing infected media.

Take precautions to protect your computer:

- Always have anti-virus software installed on your computer and make sure that it is kept up to date.
- Do not download or open an unexpected, attached email file. In addition, scan all attachments before opening.
- Never open a file or portable storage that you received without first scanning for viruses with an updated anti-virus utility.

- Do not install software – commercial, shareware, freeware or peer-to-peer file sharing products on your workstation.
- Before you open an attachment, run it through the anti-virus scanner.
- Immediately report any suspicious attachment and virus to the Campus Support Desk, 513-558-6949.
- Users with infected machines should immediately contact the Campus Support Desk, 513-558-6949, and request assistance in removing the infected file if needed.

College Wide Protection

- **Scanning Internet traffic** – All Internet traffic coming to and going from the University network is monitored for suspicious traffic. Any suspicious traffic into the UC network is blocked. This includes email messages that are believed to contain spam or phishing attempts. However, due to the constantly changing internet traffic and volume of data/emails received some of these emails and traffic will make it through the firewall.

- **Server anti-malware software** – All of UC Clermont's servers run anti-malware software. The virus definition files are automatically updated daily to ensure that the software recognizes the current virus signatures.

- **Workstation anti-malware software** - Trellix anti-malware software is installed on every UC Clermont owned computer. The workstation virus definition files are updated routinely as updates become available on the Trellix ePO server. This is completed with no user intervention required. If Trellix finds something suspicious, it is set up to automatically notify the user and attempt to clean the infected file. If the file cannot be cleaned the file is automatically deleted.

Use of Information Technology

http://www.uc.edu/content/dam/uc/infosec/docs/policies/Use_of_Information_Technology_Policy.pdf

Contacts

Campus Support Desk 513-558-6949

History

Created 11.16.2016
Amended 1.23.2023