

Columbus State University

Virus Protection Policy

Revised 3/18/2014



1.0 Background

A computer virus is a program designed to spread itself by infecting program files and making copies of itself. Viruses usually operate without the knowledge of the user and can be very destructive not only to the personal computer, but to the entire network. Protection against viruses and other malicious code is an important component in providing for the confidentiality, integrity, and availability of CSU's information assets.

2.0 Purpose

This policy defines virus protection standards and best practices for CSU computers. Users may also follow these guidelines to protect their personally owned computers.

3.0 Policy

All CSU computers, including file servers, must utilize virus detection software. Non-CSU computers that connect to CSU resources must utilize virus detection software.

Virus scanning of all inbound e-mail messages is required.

Users must not open e-mail attachments from unknown sources.

4.0 Procedures and Responsibilities

UITs personnel will install McAfee Total Protection software on all campus computers prior to distribution. This software updates its virus engine and definitions automatically.

Although UITs does not install software on personally owned computers, UITs will provide anti-virus software recommendations.

Systems administrators are responsible for anti-virus software running on CSU file servers. This includes installation, maintenance, reporting, and investigation.

Users must report suspected virus infections immediately to the UITs Help Desk.