Antivirus Software Policy

0.0 CONTENTS
1.0 Purpose and Justification
2.0 Requirement to Use Antivirus Software
3.0 Considerations
4.0 Path for Development and Approval
5.0 Timetable
6.0 Current Standards

1.0 PURPOSE AND JUSTIFICATION

The purpose of antivirus software is to provide the College of Charleston community with comprehensive protection against computer viruses and malicious code. This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files and hardware. In addition to protecting the information on individual desktop computers and servers, antivirus software protects the campus network. The availability, performance, and security of the network represent essential core assets to the daily operation of the College of Charleston. Viruses and other forms of malicious code (worms, trojans, backdoors, VBS scripts, mass-mailers, etc.) represent a significant threat to these assets.

2.0 REQUIREMENT TO USE ANTI VIRUS SOFTWARE

The Departments of Academic Computing and Administrative Computing and Telecommunications (ACTS) are responsible for supplying a campus wide license for antivirus software. All faculty and staff desktop computers and server computers connected to the campus network must have up-to-date the antivirus product installed and running. Exceptions will be allowed only when the installation of antivirus software causes conflicts with specialized, discipline-specific software. The exceptions should be approved by the network security administrator in ACTS.

Antivirus activities must be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. The Department of Administrative Computing has the responsibility for installing and updating antivirus software on desktop computers in faculty and staff offices and on servers that it maintains. The Department of Academic Computing has the responsibility for installing and updating antivirus software in student computing labs, classrooms, the library and on servers that it maintains. Generally antivirus software is distributed using deployment software.
All faculty, staff and server computers connected to the campus network shall have an up-to-date antivirus product installed and running. Services operating on servers that have antivirus products available shall have them installed. For operating systems that have no supportable antivirus products, all security patches shall be applied. All computers must meet minimum hardware requirements.

At present there is no technical support for students comparable to that given faculty and staff. Nevertheless, it is extremely important that students in the residence halls and elsewhere accessing the campus network use up-to-date antivirus software. All users must be continually educated about viruses and the computing practices required to protect against them. Whenever a new threat appears, the user community must be warned about the new threat. Up-to-date antivirus software is distributed to students and others via the website (http://antivirus.cofc.edu) and its availability advertised to the College of Charleston community.

3.0 RESPONSES TO A VIRUS INFECTION

3.1 Helpdesk must be contacted immediately when a computer has been infected with a virus. See Policy #4 for Helpdesk response time commitments.

3.2 Normally, a technician will be able to remove the virus. This may involve a visit to the work site or resolution may take place remotely if the technician can access the computer using screen-sharing software. If a technician is unable to remove a viral infection, the computer's hard drive must be reformatted and all software reinstalled using clean, licensed copies.

3.3 If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer will be immediately disconnected from the campus network until it is serviced by a technician who will then verify that the computer is virus-free.

Sponsor: C. Zeberlein
Reviewed: DAC/DACTS
Reviewed: ITSC
Reviewed: FETC
Recommended: DAC/DACTS
Approved: Provost/Senior Vice President

July 2002
July 2002
October 2002
December 10, 2002
March 2003
March 2003