WASHINGTON STATE UNIVERSITY
EXECUTIVE POLICY MANUAL
Executive Policy #14
Approved February 4, 2002

University Antivirus Policy

PURPOSE

Washington State University shall promote a secure computing environment for all students, faculty, staff and affiliates. Computing platforms (including but not limited to: desktop workstations, laptops, hand-helds, personal digital assistants, servers and network devices) are integral elements in the operations of the University and as such are vital to the University's mission. Computer viruses, worms, trojans, etc. constitute a major threat to the integrity and performance of the computing operations on campus, including access to critical data and the availability of the campus network. This policy will help ensure that all vulnerable computing platforms on campus are hardened against attack and protected by antivirus software at all times.

ANTIVIRUS SOFTWARE POLICY STATEMENT

Any computer or network device connected to the WSU network shall be protected by antivirus software from malicious electronic intrusion. This policy applies to all devices connected, by any means, to the WSU network including those owned by the University, private individuals such as faculty, staff and students, affiliates, and third-party vendors, as well as any systems obtained through grant funding.

SYSTEM HARDENING AND ANTIVIRUS SOFTWARE MANAGEMENT

Any computer or networked device that is connected to the campus network by any means, including wireless or dial-up connections, must be hardened against attack by viruses, worms and trojans. All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network and within seven days of their availability on the vendor's web site thereafter. Additionally, those systems for which antivirus software is available shall have it installed and configured for effective operation prior to their connection to the campus network. Mail Servers must be configured with antivirus software that disinfects all incoming and outgoing electronic mail and attachments.

Unit administrators, system administrators, individual computer users such as students, faculty, staff, affiliates and third-party vendors are individually and collectively responsible for the antivirus software and applicable operating system and software patches for devices under their control. For privately-owned devices connecting to the campus network, this responsibility lies with the primary user of that machine.

All antivirus software shall be actively managed to ensure that the latest software updates and the virus signatures are installed. It is strongly recommended that the antivirus software be configured to obtain these updates automatically and frequently from either the antivirus vendor, from a central departmental location or campus-wide source.

The University reserves the right to review any device attached to the network (public or non-public) for adequate virus protection. The University reserves the right to deny access to the network to any device found to be inadequately protected. Additionally, the University reserves the right to disable network access to any device that is insufficiently protected, or currently infected with a virus. Network access may be restored when the device has been cleaned and current antivirus software and applicable operating system and application patches have been installed