

Title of Policy: Antivirus Software Policy

Purpose of Policy: To prevent infection of UMass Lowell computers and networks by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to University assets such as the network, user applications, files, and hardware.

Applies to: *Any user connecting a PC or laptop to the UML network*

Person with Primary Responsibilities: IT Security Specialist

Approved: Vice Chancellor of Information Technology

Revised: 11-August-2008

Policy Statement

All Windows and Macintosh computers (clients and servers) connected physically, ***wirelessly*** or remotely (***for example, via VPN***) to the UMass Lowell network shall have antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.

To prevent viral propagation to other networked devices or harmful effects to the network, computers infected with viruses, worms or other forms of malicious code, may be disconnected from the network until the infection has been removed.

If feasible, all departmental servers providing email services shall direct all inbound email through the campus antivirus scanners at the Internet gateway. This is done by creating a Mail Exchange (MX) record in the campus primary DNS. Once email is scanned, the antivirus scanners will relay the email to the respective email server for delivery.

Accountability

Deans, Department Chairs, and Directors are responsible for monitoring compliance with this policy and associated standards by:

- Directing administrators of Windows and Macintosh machines in their respective departments to install approved or comparable antivirus software on desktops, laptops, and servers connected to the University network.
- Directing reviews of and action on, reports on compliance with this policy that are generated by campus IT Security and related support services.

Individual users (faculty, staff, and students) are responsible for compliance with this policy and its associated standards for departmental and personally owned machines (including laptops/notebooks) connected to the University network.

Installation Requirements:

If a Windows or Macintosh computer does not have antivirus software installed, it shall be installed according to one of the two following methods:

- If the installation source is a University-distributed CD-ROM, the antivirus software shall be installed before establishing any connection to the network. Upon establishing the

initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.

- If the installation source is a University server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately upon establishing the initial network connection and virus updates downloaded and installed before loading or installing any other software or data.

Under all other circumstances, any Windows or Macintosh computers connected to the network shall have antivirus software properly installed, configured, and updated before being connected to the network. **Under no circumstances should any computer connect to the network if a virus has been detected and cannot be removed by AV software.** At a minimum:

- Virus definitions **shall be updated daily**
- All files on all hard drives shall be scanned daily (**preferably scheduled**) at a time convenient for the user.

When an enterprise-wide virus attack is in progress, IT Security shall notify the campus computing community via the best available method, and all files on all hard drives should be scanned immediately using the newest virus definitions available.

Other operating systems (Unix, Linux) shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

The IT Security Specialist must explicitly approve any exceptions to this policy and respective workarounds.

Justification and Rationale

Availability, performance, and security of the network represent essential core assets to the daily operation of the University. Viruses and other forms of malicious code (worms, Trojans, backdoors, VBS scripts, mass-mailers, etc.), represent a significant threat to these assets. In order to combat this threat, a comprehensive enterprise security policy must include antivirus provisions to detect, remove, and protect against viral infections.

Many virus infections threaten other computers sharing the infected computer's network. Files that can be cleaned should have the viral code removed -- returning them to pre-infected state. Files that cannot be cleaned must be quarantined until such time as they can be replaced with uninfected copies. If all efforts at removing viral infection fail, the computer's hard drive must be formatted and all software reinstalled using clean licensed copies. If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer must be disconnected from the network until it is serviced by a Desktop Support Services representative or designee who will verify that the computer is virus-free.

Antivirus activities should be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. Users must be educated about viral threats and best practices required to protect against infection. Whenever a new viral threat appears, the user community must be warned about the new threat. Up-to-date antivirus software must be distributed and its availability advertised to the University community.

Established Antiviral Procedures:

UMass Lowell has taken a multi-tiered approach to address computer viruses. For the approved primary email servers on campus (MS Exchange), all inbound email is scanned by a series of antivirus/antispam network scanning appliances. For the desktop and servers, the University has a site license for McAfee VirusScan Enterprise. The site license permits UML faculty, staff, and students to have VirusScan on all Windows and Macintosh computers on the UML campus. The site license also contains provisions allowing UML faculty, staff, and students to install VirusScan Enterprise software on their home computers free of charge.

Computers purchased for large-scale rollouts are delivered with McAfee VirusScan Enterprise already installed. Whenever Desktop Support Services configures a new computer, they ensure that McAfee VirusScan Enterprise is installed before or immediately upon connecting the computer to the network. IT Support Services distributes the McAfee VirusScan software as follows:

- Campus users can request McAfee VirusScan installation on campus computers by contacting the Help Desk (ext 4357).
- On-campus users can install McAfee VirusScan from the Support Services website located at <http://antivirus.uml.edu>

Comparable Antivirus Software:

Departments and students that have purchased comparable anti-virus software (e.g. Norton, TrendMicro, Sophos) must ensure the software is properly licensed, installed, configured, activated and updated with the latest version of virus definitions before or immediately upon connecting to the network. New computers often have trial versions of AV software which expires after a short period of time, be sure to renew the license upon expiration or install an All provisions of this policy apply to comparable anti-virus software.