

UMB, UMMC, UPI and SOM Enterprise Anti-Virus Policy

Updated: 2/20/04

Effective Date: 3/25/04

Executive Summary

Incorrectly configured or absent anti-virus software on campus workstations and servers has become one of the greatest threats to the campus network community. It is imperative that we take a proactive approach in making sure that all computers connected to the campus network are properly configured and protected with anti-virus technology. It is equally important that we proactively monitor campus networks for non-compliance.

Goal

The goal of this policy is to protect every piece of computer equipment from infection by viruses, worms, trojans, and other malicious software. Threats from these vectors are so severe that it is mandatory for every computer to be protected from them continuously. This policy will provide the rules and guidelines that govern anti-virus use on all computers connected to the University of Maryland Baltimore campus network.

Scope

This policy applies to both end users and designated IT technicians.

- End users are responsible for alerting campus IT organizations to the attachment of computer equipment to the network and for permitting campus technicians to install and fully manage approved anti-virus software on that equipment.
- Technicians designated by campus IT leaders are responsible for installing, configuring and managing anti-virus software on all computers attached to the network in accordance with the following standards.

This policy applies to all desktops, laptops, workstations & servers (referred to throughout this document as “**computers**”) connecting to the campus network.

General Policy

Anti-Virus software must be installed on all campus computers. While the campus cannot define a specific vendor as a requirement, it has defined the minimum requirements that must be met when choosing an anti-virus software vendor. Therefore, it will be the responsibility of each entity to provide an anti-virus solution that best suits their business needs while meeting the campus anti-virus software requirements. That solution must also allow for all computers connected to any segment of the campus network to implement the following virus protection controls.

Anti-Virus Vendor Guidelines

Software capabilities:

- Anti-Virus software must be able to be automatically installed at user logon.
- Anti-Virus software must be manageable from a central console server.
- Anti-Virus software management central console servers must be able to distribute virus definition files and product updates.
- Anti-Virus software console must provide real-time status of all client workstations, inclusive of software version and signature file release date.

- Anti-Virus software must support automatic updating of virus definition files.
- Anti-Virus software must support automatic scanning of computer system on a regularly scheduled basis.
- Anti-Virus software must support end user restrictions.

Specific vendors that meet this policy's requirements will be listed under the guidelines section.

Approved Anti-Virus Vendors

1. Symantec AntiVirus Corporate Edition
2. Network Associates – McAfee VirusScan Enterprise

Perimeter Security:

- All incoming campus SMTP traffic must pass through campus anti-virus gateway filters managed by UMB.

Installation and Configuration

- All campus SMTP servers must have anti-virus agents installed to scan incoming email.
- An employee designated by the institution will install, configure and manage anti-virus software.
- Anti-Virus software must be installed immediately upon user login if not already installed.
- Anti-Virus software must be configured to update virus definition files once daily
 - Central console servers must be configured to get updates from either a vendor specified location or campus specified location.
 - Client workstations must be configured to get updates from its central console server.
- Anti-Virus software must be maintained at a level whereby the latest installed version for the major scan engine is no more than 2 revisions old.
 - Anti-Virus software scan engines must be obtained from either a vendor specified location or made available at a campus specified location.
- Anti-virus software must be maintained at a level whereby the latest installed virus definition files are no more than 2 weeks old.
- Anti-Virus software must operate continuously when the computer is running.
- Anti-Virus software must be configured to run checks for viruses at least once per week and operate in memory-resident mode at startup to check for viruses during normal processing.
- Anti-Virus software must be restricted so that configuration settings cannot be changed or disabled by the users.
 - Restrict access to real time protection settings,
 - Restrict the ability to unload from memory
 - Restrict un-installation by changing the default uninstall password.
- Anti-Virus software must not unduly interfere with the approved normal uses of the computer.
- Personal computers brought from home or by vendors and/or business associates must have institutionally approved anti-virus software installed with recent (within one month) virus definition files before they will be allowed to connect to any campus network segment.

- Workstations used from home for remote access must have institutionally approved anti-virus software installed with recent (within one month) virus signatures before they will be allowed to connect to any campus network segment.
- Anti-Virus software installation and configuration documentation must be maintained for each departmental installation.

Auditing and Monitoring

- Workstations must be able to be audited by the central console server to determine if the workstation has protection & is up to date.
- The central console server must audit workstations in real-time. This is to say that the central console server is in constant communication with the client.
- Campus network services will monitor both central console servers and workstations under their control for up to date virus signatures and engines.
- Campus network services may perform network scans for devices that do not have anti-virus software.

Contingency Planning

Outbreak Management

Central console server administrators must supply local network administrators the logon information for their central console servers as well as any emergency contact information. This information must be updated regularly to avoid a communication breakdown during an attack .

Campus network services have the discretion to segment local network traffic in response to malicious attacks if necessary and approved by their respective CIO.

Incident Response Procedure

An incident response plan needs to be defined. This plan should include who and how communication of an outbreak is handled.

Business Requirements for Disabling Anti-Virus software

Departmental administrators will have discretion to disable anti-virus software for valid business reasons. Notification must be sent to local campus network services of this decision.

Anti-Virus Software Updates

Campus network entities will maintain master live update servers with the latest updates. In the event of a disruption in Internet connectivity, these servers will be manually updated to provide the latest scan engines and virus definition files to internal campus anti-virus console servers. Location and logon information of these servers must be published so that all campus IT administrators can quickly configure access from their respective console servers.

Technical Support

Departments must maintain the ability to contact vendor support for their anti-virus products, which include both online and phone support.

Communication

End User Responsibility

It is the responsibility of the end-user to notify their local network group immediately when a new computer is physically connected to the network, when anti-virus protection software appears to be malfunctioning or when they believe a computer might have become infected. The network group will determine the appropriate department or group to install anti-virus software or mediate the risk.

IT Technician Responsibility

New anti-virus servers must be communicated to the local network administrators.

Outbreak Communication

Any type of virus or malicious software event must be communicated to the 4 main campus network services, which then will disseminate the information to their departmental administrators. Information must include virus name (if known) and OS level. Information may need to be forwarded through use of voice mail and/or fax as well as email.

Effective Date

Installation and configuration of anti-virus software in accordance with the approved standards must commence immediately upon executive approval of this policy.

Violations

- Failure to notify the appropriate parties of new computers needing anti-virus software is a violation of this policy
- Failure to install and operate approved anti-virus software is a violation of policy.
- Disabling, circumventing or tampering with anti-virus protections and/or software constitutes a violation of policy.
- It is the responsibility of each departmental IT administrator to make sure that they are keeping their departmental systems updated with the latest anti-virus signatures and protection. Failure to do so constitutes a violation of policy.

Enforcement

Violations in policy could result in progressive disciplinary action dealt with through normal disciplinary processes within each organization.

In the course of monitoring, any computers found not to be in compliance will be disconnected from the network until they can be properly configured.

Revisions

As the nature of viruses, worms and trojans change, and technology improves, this policy will be reviewed and revised as necessary.