

SMNSFD – State of Maryland Network Security and Forensics Department

Title of Policy: Antivirus Software Policy

Purpose of Policy: In order to prevent infections through state and local information technology infrastructures, strict policies must be developed and adhered through utilizing this mandate. Personnel responsibilities are clearly defined and outlined to assist in Business Continuity Planning.

Applies to: All personnel, state buildings, public facilities, and government programs within Maryland's state lines.

Person with Primary Responsibilities: Systems Security Officer(s) throughout each and every district.

Approved: Director of Operations

Date: 09/01/05

Policy Statement

All client and server systems connected physically or remotely to the State of Maryland's various infrastructures shall have correctly monitored and patched Symantec AntiVirus Enterprise Edition™ software installed, configured, and updated before connecting to the network(s).

In order to combat wide-spread outbreaks, if necessary, systems infected with viruses, worms, malicious code, or other various forms of exploits shall be disconnected from the network until the infection has been mitigated.

Each mail server shall have monitoring provided by Symantec Mail Security™ for Microsoft® Exchange installed and monitored by an appointed Exchange Mail Administrator and verified by a Systems Security Officer.

Each web server (IIS based) shall have active monitoring provided by Symantec Web Security™ installed and monitored by an appointed Web Applications Administrator and verified by a Systems Security Officer.

Accountability

The Director of Operations and each facility's Systems Security Officers are directly and solely responsible for maintaining a high-level of compliance with this mandated policy by:

- Appointing the appropriate administrators to install, verify, and maintain updated antivirus systems.
- Initiating auditing procedures as part of the interim quarterly reporting.
- Individual users (directors, managers, staff, interns, and third-party affiliates) are responsible for compliance with this policy and its associated standards for departmental and personally-owned machines connected to the State's network.

Installation Requirements:

If a client or server computer does not have antivirus software installed, it shall be installed according to the following method:

If the installation source is a server maintained for the purpose of antivirus installation, 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 initializing network connection. All antivirus updates must be downloaded and installed before loading or installing any other software or data.

Under supervision and monitoring the following should be maintained at a minimum:

- Virus definitions shall be updated **daily**.
- All files on all hard drives shall be scanned daily at a convenient time for the end user.
- Active monitoring shall be enabled with capabilities to disable active monitoring administratively removed.

When an systems-wide virus attack is detected, Administrators shall notify the designated Systems Security Officer via the best medium available (whether it is phone, page, email, or text message), and all files on all hard drives should be forcibly scanned immediately using the newest virus definitions available for download and implementation.

Other operating systems shall have comparable protection, if available. If no antivirus protection is available for a particular operating system, anyone using or accessing these unprotected systems shall apply best 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 previously lacking antivirus software, it shall be installed on all systems connected to the network.

The Director of Operations is responsible for amending and maintaining these procedures to eliminate undefined incidents and documentation loopholes.

Justification and Rationale

The high-availability, dependability, and security of the network infrastructure is essential to the business continuity of the State of Maryland's Network Security and Forensics Department as well as other vital State-funded and operated networks. New ever changing threats loom over our technology and adaptable software is needed to maintain a sense of order and safety.

The antivirus software should be intelligent and sufficient not to eliminate the infected files that may maintain critical data. If the infection cannot be dealt with, the software should have the ability to quarantine the data until an appropriate action can be decided by the designated Systems Security Officer.

The most crucial aspect that the antivirus software should have is central management to push out updates as well as keep detailed records of virus activity.

Among other software-related topics, an essential step must be education to both the staff and end-users. Without proper education of the dangers of email attachments, peer-to-peer file sharing, and internet downloads, we fight a losing battle against new threats and vulnerability.

Established Antiviral Procedures

The State of Maryland has taken a multi-tiered approach to dealing with antiviral removal and prevention. Multiple products – listed above – maintain our systems while chain-of-command maintains watch guard that this policy. We maintain 1000 active licenses for our software to well-accommodate our staff's needs, with the ability to add more, by requisitioning the Director of Operations.

Whenever a new computer is configured, antivirus software must be installed before or immediately upon connecting the computer to the network. Antivirus software is only distributed via the following methods:

- Administrators are permitted install it on clients and servers through network installation.
- New system installations may be installed offline only by written permission by Director of Operations.
- Only official State maintained and owned systems are permitted to install services.

