

STATE OF VERMONT
Agency of Administration

| | | |
|---|--|---|
| POLICY STC STATE TECHNOLOGY COLLABORATIVE | Final | ORIGINAL POLICY NUMBER 0502.012005 |
| | EFFECTIVE DATE Upon Approval | ASSOCIATED DOCUMENTATION Malicious Software Protection Standard |

STATUTORY REFERENCE
OR OTHER AUTHORITY:

**State of Vermont Personnel Policies and Procedures Number 11.7 -
Electronic Communications and Internet use –
<http://www.state.vt.us/pers/er/pm/pm117.htm>**

APPROVAL DATE:

APPROVED BY:

Secretary of Administration

POLICY TITLE:

Malicious Software Protection for Desktops & Servers

POLICY STATEMENT:

Anti-virus / Anti-Malware applications, protecting PC based systems, are one of the most effective protections against the damage caused by malware. All PC based computers in use by the State of Vermont, or accessing non-public SOV resources, must have current, active malware protection.

POLICY PURPOSE

The purpose of this policy is to establish a requirement for the protection of the State of Vermont's IT environment from viruses and other malicious software that are commonly called malware.

POLICY SCOPE

This policy applies to all agencies, departments, and other entities including third-party business relationships that require access to non-public SOV resources. This includes, but is not limited to, desktop computers, laptop computers, proxy servers, and any file and print servers. In addition, all e-mail gateway providers must provide malware checking and protection for email messages processed by the gateway.

Policy:

Malware protection must be provided throughout the IT environment in the State of Vermont. The appropriate level of protection continually evolves based on the threats and the available solutions. The associated standard defines the appropriate level of protection.

Responsibilities:

Agencies or Departments are responsible for:

- Creating procedures that ensure anti-malware software is installed, routinely updated, and operational.
- For ensuring that computers are verified as malware free.
- For removing computers that are infected with malware from any network.
- For ensuring that computers remain disconnected from any network until they are verified as malware free.
- Ensuring that any activity by their employees conform to this policy and its related standards.

Enforcement:

Routine monitoring of networks can provide patterns of non-standard traffic that are indicative of many types of malware. Upon becoming aware of this type of traffic, the Department of Information and Innovation (DII) staff will notify the designated IT contacts or the head of the agency of the offending device. If after a reasonable time, the offending device is not removed from the network, DII staff is required to eliminate the offending behavior in the least impacting manner that meets the goal of protecting the rest of the network.

At their discretion, DII staff are empowered and encouraged to conduct audits of any PC systems that fall under this policy. This type of audit may be triggered when patterns of problems indicate that it is likely that associated standards for this policy are not being met.

Any employee found to have knowingly violated this policy may be subject to loss of privileges and /or disciplinary action, up to and including termination of employment. As stated in personnel policy and procedures 11.7.

APPROVED

Secretary of Administration

Date