

Information Technology Virus Protection Policy

Objectives

The principal concern of this computer virus protection policy is effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with Saint Michael's College. Our goals are to ensure that SMC-affiliated users (faculty, staff, and students, and visitors) are aware of and take responsibility for the proper use of the College-provided and Information Technology supported virus protection software. This policy is intended to ensure:

- ♦ the integrity, reliability, and good performance of college computing resources;
- ♦ that the resource-user community operates according to a standard of safe computing practices;
- ♦ that the College licensed virus software is used for its intended purposes; and
- ♦ that appropriate measures are in place to reasonably assure that this policy is honored.

Policy

Centrally provided virus protection software will be run on all Saint Michael's College computers and on all computers connected to the Saint Michael's College Network. 

Goals

- ♦ Prevent all infections. And when that is not possible, create an outlet for notification and annotation of virus outbreaks for College service providers and end-users so that future breaches can be prevented.
- ♦ Prevent the loss of information/data and software on College-owned computers and minimize the cost of computing maintenance and network downtime by virus outbreaks.
- ♦ Distribute updates of virus protection software and other important campus-supported software to all College-affiliated computer users. Virus protection software that is not used cannot prevent infections.
- ♦ Create a system for, immediate notification of the VPT and the AU user community once an outbreak has been detected.
- ♦ Annually evaluate the number of virus outbreaks to determine whether this policy and the College-provided virus protection software are still valid and appropriate.
- ♦ Provide and continue to support the best virus protection solution that the Saint Michael's College campus can support.
- ♦ Require a minimum of end-user responsibilities in regard to computer virus protection practices.

Compliance

Virus protection is most effective if every computer on the Saint Michael's College network has anti-virus software installed and is actively monitoring network activities. IT staff will 1) provide the initial setup for campus computers; 2) distribute virus protection updates. The anti-virus software will be available for SMC-affiliated users to install on their computers IT staff will provide assistance in removing existing anti-virus programs from campus computers.

- ♦ IT will monitor network activity and initiate appropriate action to control infection. We reserve the right to disconnect any server or client known to be an infecting agent. Such a disconnection is an **emergency** action.
- ♦ The user will be contacted immediately, and IT will work with the user to solve the problem.

Information Technology Virus Protection Policy

IT Responsibilities

- ◆ Acquire the licenses for anti-virus software
- ◆ Procure software and updates from the vendor, as they are made available.
- ◆ Expediently make the software and updates available to College service providers and users.
- ◆ Configure software for distribution in accordance with current SMC policy.
- ◆ Provide documentation for users.
- ◆ Provide a central repository of information regarding infections by viruses of College owned computers allowing effective reporting and analysis.

End-Users

Computer systems owned by Saint Michael's College will run anti-virus software, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Responsibilities

- ◆ Install and maintain current virus protection software
- ◆ Be certain that the software is running correctly. If these responsibilities appear beyond the end-user's technical skills, the end-user is responsible for seeking assistance from IT.
- ◆ Perform regular backups. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Noncompliance

- ◆ SMC faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections, which could result in:
 - ◆ damaged or lost files
 - ◆ inoperable computer resulting in loss of productivity
 - ◆ risk of spread of infection to others
 - ◆ confidential data being revealed to unauthorized persons
- ◆ An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole colleges. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

Distribution

IT is responsible for distributing the software for initial installation and subsequent updates. Although the distribution mechanism depends in part on the specific virus protection software acquired by the College, most include the following distribution methods:

- ◆ scheduled, unattended updates by the client via FTP, Web, or propriety agent.
- ◆ attended updates initiated by the user of the client via FTP, Web, or propriety agent.
- ◆ scheduled, unattended updates initiated by the server via FTP, Web, or propriety agent.
- ◆ Unless there is a compelling rationale otherwise, all updates will be scheduled. Further, if distribution mechanisms allow, the server providing the highest level of protection will initiate updates.
- ◆ Server-initiated updates will normally be timed; however, in the event of a virus outbreak, updates can be pushed to client computers without intervention by the user.

Our policies are designed to reflect current conditions. As conditions change, we will review our policies accordingly; consistent with the goals of the college and subject to the availability of financial resources.
