Title:	**ANTIVIRUS GUIDELINES**
Updated:	March 12, 2012
Audience:	All internally connected labs, computer systems, employees and third parties who access the Faculty of Medicine's network
Purpose:	To ensure all systems are protected with appropriate measures in order to provide a trusted, collaborative environment for networked users
Contact:	MedIT

1 Purpose

With the widespread and rapid proliferation of viruses, worms and Trojan software being distributed on the Internet, unprotected systems are at risk of compromising the integrity of the community of users on a trusted network. It is therefore necessary to ensure all systems are protected with appropriate measures in order to provide a trusted, collaborative environment for networked users.

2 Scope

These guidelines apply to all internally connected labs, computer systems, employees and third parties who access the Faculty of Medicine's network. All existing and future equipment, which fall under the scope of these guidelines, should be configured according to the referenced documents. Stand-alone, unconnected networks are exempt from these guidelines.

3 Guidelines

To protect yourself, and your colleagues, up to date antivirus software must be installed on all desktop systems in the Faculty of Medicine network. Because new viruses are discovered almost every day, anti-virus signature files must be updated at least once per week to minimize the risk of infection with a new virus.

4 Roles and Responsibilities

All networked users are responsible for minimizing the risk of their desktop system infecting other systems or shared files on a server. Despite the best measures, systems can still be at risk due to the rapid proliferation of malicious code via email, shared files and other methods. Therefore, in addition to maintaining up-to-date antivirus software, consider the following best practices:

- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source (or if you unexpectedly receive an attachment from someone you know). Delete these attachments immediately.
- Delete spam, chain, and other junk email without forwarding it.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a need to do so.
- Always scan a floppy disk from an unknown source for viruses before using it.
- Routinely scan your hard disk for viruses; preferably on a daily basis.

Email systems with gateway antivirus software are preferred to minimize the risk of downloading a new virus to the desktop. Risk to viruses arriving via email is minimized if antivirus software is employed using a three-layered defense: at the SMTP relay transferring email from the Internet to the mail server, at the email server, and at the desktop.

5 Compliance

To protect other users, systems found to have out of date antivirus software may be removed from the network until they are maintained properly under these policies.

6 Definitions

Anti-virus software: software designed to detect, protect and remove viruses, worms, trojans and related software.

Anti-virus signature files: files provided on a regular, usually weekly basis, by the manufacturer to supplement anti-virus software so that it recognizes recently discovered viruses, worms and related code that might otherwise not be detected. Signature files must be updated frequently on the workstation to ensure anti-virus software provides sufficient protection.

Computer virus: programs or bits of code that attempt to replicate themselves from computer to computer. While in most cases they are not destructive, they may cause unusual system behavior and make changes to systems to enable them replication elsewhere. Some viruses may contain destructive code which may cause permanent damage to computer systems. Rapid replication of viruses during a severe outbreak through email can also put a severe strain on email servers that may cause performance to degrade significantly or fail.

Computer Worms: are similar to viruses, however, they are generally more destructive as they integrate themselves into existing applications, often at the operating system level, so that they behave differently from their original design.

Computer Trojans: software with possibly attractive features that would lead users to download and install it on their system, but with hidden features that may also function in a manner unknown to most users. In some cases these features may open the system to distribute confidential data or allow unauthorized access to the networked computer.

Spam: unwanted or “junk” e-mail messages, usually sent in large quantities to users placed on distribution lists without prior consent.

7 Procedures

Antivirus installation: refer to instructions provided by the software manufacturer. We currently recommend Symantec Norton Antivirus. Site licenses for this software is available at educational rates through UBC IT.

Detection of virus and related code: In most cases, up to date antivirus software will display a warning message, and then automatically handle removal of the virus/worm if it is inadvertently uploaded to your system. When complete, do a full scan of your system to ensure other files have not been infected.

Resolving suspected infections by viruses and related code: Systems that have been infected may display a wide range of symptoms. These may include anomalous behavior when running applications, unusually slow performance, or in extreme cases, complete system failure. If you suspect your computer may have been infected, stop using it immediately. Isolate it from the network by disconnecting the network cable/wireless connection before investigating it further. This will help to limit the possibility of a worm or virus spreading to other networked systems before it has been resolved. Take special care when manually removing a virus or worm from your computer to prevent further system damage and limit the possibility of re-infection at a later date. This is particularly important as in some cases a worm may allow additional software to be installed and exploit your system that may not be detected by antivirus software. If in doubt, contact a qualified systems support specialist for assistance.