Stony Brook University

Computer Science

Guidelines on Anti-Virus Process

CS Department Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

Always run the CS dept standard, supported anti-virus software that is available from the CS department download site. Download and run the current version; download and install anti-virus software updates as they become available.

Many anti-virus programs can update their definitions daily. Your anti-virus installation should be setup to check for new virus definitions at system boot.

NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

Delete spam, chain, and other junk email without forwarding, in compliance with the CS department's *Acceptable Use Policy*.

Never download files from unknown or suspicious sources.

Avoid direct disk sharing with read/write access unless there is an absolute requirement to do so.

Always scan a floppy diskette for viruses before using it.

Back-up critical data and system configurations on a regular basis and store the data in a safe place.

If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Do not run ftp or IIS services on your PC. Use ssh daemon to allow sftp access and never allow anonymous access.