

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- Always run the Corporate standard, supported anti-virus software is available from the corporate download site for home <http://antivirus.appstate.edu>, and for work please use Zenworks Application Explorer. Download and run the current version; download and install anti-virus software updates as they become available. This is accomplished automatically when user logs in to the RCOE network and will update DAT files every 3 hours.
- 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 with Appalachian State University *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a peripheral such as a flash drive from an unknown source 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.