

**Anti-Virus Guidelines**

**Purpose**

This policy *was created by or for the COMPANY\_A for the Internet community*. This policy is intended to help prevent damage to user applications, data, files, and hardware.

**Scope**

This policy applies to all employees as well as contractors, collaborators and any others doing business with the COMPANY\_A will be subject to the provisions of this policy.  Any other parties, who use, work on, or provide services involving COMPANY\_A computers and technology systems will also be subject to the provisions of this policy. Every user of COMPANY\_A computer resources is expected to know and follow this policy.

**Definitions**

Computer devices are any type of device connected to a network that could become infected with a computer virus.  Examples of computer devices would be, but not limited to, workstations, servers, laptops, PDAs, etc.

Malicious software is any type of computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, trojans, etc.

Anti-Virus software runs on either a server or workstation and monitors network connections looking for malicious software.  Anti-virus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.

Virus definition files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.

**Policy**

* Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
* 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 <Company Name>'s *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 floppy diskette 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.

**Violation of Policy**

If it is suspected that this policy is not being followed, report the incident to the Executive Associate or the Director of Technology Services.

Any exceptions to this policy must be approved in advance by both the Executive Associate and the Director of Technology Services.

**Enforcement**

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of COMPANY\_A.