**Anti-Virus Policy**

# Overview

***Anti-Virus Recommended Processes***

Recommended processes to prevent virus problems:

* 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 *Anti-Virus Policy* and this Recommended Processes list for updates.

# Purpose

To establish requirements which must be met by all computers connected to [Company Name] lab networks to ensure effective virus detection and prevention.

# Scope

This policy applies to all [Company Name] lab computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

# Policy

All [Company Name] PC-based lab computers must have [Company Name]'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into [Company Name]'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Refer to [Company Name]'s Anti-Virus Recommended Processes to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excepted at the current time.

Scanning must be completed weekly.

# Policy Compliance

* 1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

# Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

# Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Related Standards, Policies and Processes

* Acceptable Use Policy
* Anti-Virus Recommended Processes

# Definitions and Terms

None

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| July 2014 | David Veksler | Converted to new format and retired. Appropriate items merged into new Lab Security Policy. |