



Lab Anti-Virus Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

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

2.0 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.

3.0 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.

4.0 Enforcement

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

5.0 Revision History