Lab Anti-Virus Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the policy for your organization*

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

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

3. 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.

4. 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.

5. Policy Compliance

5.1 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.

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

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

6 Related Standards, Policies and Processes

- Acceptable Use Policy
- Anti-Virus Recommended Processes

7 Definitions and Terms

None

8 Revision History

Date of Change	Responsible	Summary of Change
July 2014	SANS Policy Team	Converted to new format and retired. Appropriate items merged into new Lab Security Policy.