Server Malware Protection Policy

Last Update Status: *Retired*

1. Overview

<Company Name> is entrusted with the responsibility to provide professional management of clients servers as outlined in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

2. Purpose

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

3. Scope

This policy applies to all servers that <Company Name> is responsible to manage. This explicitly includes any system for which <Company Name> has a contractual obligation to administer. This also includes all server systems setup for internal use by <Company Name>, regardless of whether <Company Name> retains administrative obligation or not.

4. Policy

<Company Name> operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

4.1 ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to this server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet

- Other "risky" protocols/applications are available to this system from the Internet at the discretion of the <Company Name> Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Outbound web access is available from the system

4.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

4.3 ANTI-SPYWARE

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

4.4 NOTABLE EXCEPTIONS

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

- The system is a SQL server
- The system is used as a dedicated mail server
- The system is not a Windows based platform

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, 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

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Malware
- Spyware

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted format and retired.