SERVER MALWARE PROTECTION POLICY

1.0 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.

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

3.0 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.

4.0 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

5.0 Enforcement:

The responsibility for implementing this policy belongs to all operational staff at <Company Name>. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the <Company Name> Security Officer. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions:

TERM	DEFINITION
Server	For purposes of this policy, a server is any computer system residing in the physically secured data center owned and operated by <Company Name>. In addition, this includes any system running an operating system specifically intended for server usage as defined by the <Company Name> IT/IS Manager that has access to internal secure networks. This includes, but is not limited to, Microsoft Server 2000 and all permutations, Microsoft Server 2003 and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to and VMS.
Malware	Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Spyware — Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Anti-virus Software — Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

7.0 Revision History:

8.0 References:

"Malware." Wikipedia, The Free Encyclopedia. 08 Nov 2006,

< http://en.wikipedia.org/wiki/Malware>

"Spyware." Wikipedia, The Free Encyclopedia. 08 Nov 2006,

<http://en.wikipedia.org/wiki/Spyware>

"Anti-Virus." Wikipedia, The Free Encyclopedia. 08 Nov 2006

< http://en.wikipedia.org/wiki/Anti-virus>