STAGES SERVER VIRUS/MALWARE SETTINGS

Description of Server Recommendations

Official Release

Version 1.0

Secure Global Solutions

www.secglobe.net

Virus and Malware Protection

Virus Protection is highly recommended and should be installed on your stages servers. While we have no recommendations with respect to a particular product or supplier, SGS uses ClamWin as part of its overall security strategy. Many of our customers have used ClamWin, Sophos, Trend Micro, ESET NOD32 and others with great success.

Outlined below are a few important points that should be observed when using Virus applications on IIS and SQL servers.

1. IIS:

You should exclude the IIS compression directory from the antivirus software's scan list.

The default compression directory in IIS 6.0 is

%systemroot%\IIS Temporary Compressed Files.

This directory may have been changed to another location. In IIS 7.0, the default location of the compressed file cache is

%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files.

To verify the compression directory:

1. Click Start, point to Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In IIS Manager, right-click the Web Sites folder, and then click Properties.
3. Click the Service tab.

Under HTTP Compression, make sure that “Compress static files” is selected, and then locate the path to the temporary directory.

The following are process exclusions, meaning that these should be excluded from the virus scan.

- %systemroot%\system32\inetsrv\w3wp.exe
- %systemroot%\SysWOW64\inetsrv\w3wp.exe

2. SQL

The following items should be excluded from virus scan.

- SQL Server data files
    - *.mdf
    - *.ldf
    - *.ndf
- SQL Server backup files
    - *.bak
    - *.trn
- Full-Text catalog files
    - Default instance:

      Program Files\Microsoft SQL Server\MSSQL\FTDATA

    - Named instance:

      Program Files\Microsoft SQL Server\MSSQL$instancename\FTDATA

- Trace files
    - *.trc

      NOTE: (these files can be generated either when you configure profiler tracing manually or when you enable C2 auditing for the server)

- SQL audit files (for SQL Server 2008 or later versions)
    - *.sqlaudit
- SQL query files
    - *.sql