

<COMPANY>

**PR04 - Anti Virus & Malicious Software Procedure**

<b>Document Reference</b>	PR04 - Anti Virus & Malicious Software Procedure
<b>Date</b>	
<b>Document Status</b>	Final
<b>Version</b>	1.0
<b>Revision History</b>	

## Table of Contents

1.	Purpose.....	3
2.	Scope.....	3
3.	Roles and Responsibilities .....	3
4.	Procedure.....	3
4.1.	Anti-Virus Software Installation.....	3
4.2.	Anti-Virus Software Testing .....	4
4.3.	Maintaining and Updating this Anti-Virus Procedure. ....	4
5.	Enforcement .....	4
6.	Definitions and References .....	4
6.1.	Definitions .....	5
6.2.	References .....	5

## 1. Purpose

Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to <COMPANY> in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of <COMPANY> is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by <COMPANY> employees to help achieve effective virus detection and prevention.

## 2. Scope

This policy applies to all computers that are connected to the <COMPANY> network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the <COMPANY> network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

## 3. Roles and Responsibilities

*Infrastructure* team - Responsible for executing and implementing this procedure.

<IT> *Manager* - Responsible for monitoring the implementation of this procedure.

See **P01 – IS Policy** for team membership.

## 4. Procedure

### 4.1. Anti-Virus Software Installation

- The <Vendor/ Product/ Version> anti-virus software is installed on all <COMPANY> desktop workstations, laptops, and servers, following the vendor installation guide provided with the software.
- The anti-virus software Console window provides complete access to the options available, although several of the most frequently used tasks can be accessed by right-clicking on the anti-virus software icon in the task bar.
- The anti-virus software includes the full version of McAfee's anti-spyware module, which protects computers from malicious software that isn't categorized as a virus. The anti-spyware module blocks spyware, adware, cookies, jokes, and Trojans.
- Note that remote administration tools are included in this list of potentially malicious software. By default, remote administration software is blocked by this program, to prevent remote administration tools allowing an attacker access to <COMPANY> systems. However, if third-party remote administration tools have been intentionally turned on, the remote administration blocker should be turned off .
- On-Access Scanning is enabled, and configured so that anti-virus software cannot be disabled on all desktop workstations, laptops, and servers. On-Access Scanning runs automatically and scans a file before opening any file accessed.
- The Full Scan option is enabled, so that the AV server will conduct a weekly scan of all workstations, laptops, and servers on the <COMPANY> network. The Full Scan item scans every file on each computer, can be memory-intensive, and take several hours to complete, and so is usually scheduled to run over the weekend. To scan a computer hard

drive(s) for viruses on an ad-hoc basis, select the Full Scan option in the anti-virus software Console window.

- Following completion of a Full Scan, the following are completed:
  - Full Scan Report review: <COMPANY> to document who receives the scan report to review it.
  - Full Scan Corrective Action: <COMPANY> to log corrective action with respect to any issues raised from the weekly scans in line with **PR05 - Change Control Procedure**.
- The Buffer Overflow Protection option is enabled, where applicable, to protect the <COMPANY> network against buffer overflow exploits.
- The Script Scan option is enabled, where available, so that scripts (Java Script and VBScript) are scanned before they are executed.
- The Scan Email option is configured, where available, to enable the Microsoft Outlook/Lotus Notes Email Scanner option.
- The Access Protection can optionally be enabled, where available, to act like a limited firewall, permitting blocking of specific selected networking ports.
- Antivirus software is configured for regular updates to catch new viruses. This is achieved by ensuring that the anti-virus product is updated in terms of both virus definitions (DAT) files and the scan engine version being used.
  - The AV server is configured to check the vendors website for updates *twice daily*; other servers and workstations automatically check the AV server for updates *twice daily*. <COMPANY> laptops are configured so that VirusScan will check the AV server for any new updates *twice daily* and if they can't reach the AV server, are updated directly from the vendor website.
  - If any machine fails an AV update: <COMPANY> to document whenever any machine(s) fail to update, who is informed, and details of the corrective action taken.
  - The scan engine version patches are installed onto the AV server manually from the vendor website, and after being successfully tested, are installed automatically onto all other <COMPANY> servers and workstations.

#### 4.2. Anti-Virus Software Testing

- After installation, and optionally at periodic intervals, the anti-virus software must be tested following a vendor approved test regime to ensure the anti-virus software can properly scan for potentially unwanted programs. An example of a vendor approved test regime is the test developed by the European Institute for Computer Anti-Virus Research (EICAR).

#### 4.3. Maintaining and Updating this Anti-Virus Procedure.

- <COMPANY> is to define the process followed to periodically update this procedure, including the version control applied, and any auditable materials generated.

### 5. Enforcement

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

### 6. Definitions and References

---

<COMPANY>  
Form Name : PR04-  
Antivirusmalicioussoftwareprocedure  
Version :  
Date Last Updated:

COMMERCIAL IN  
CONFIDENCE

Page 4 of 5

THIS DOCUMENT IS UNCONTROLLED IF PRINTED OUT OR IF NOT VIEWED AS PART OF THE <COMPANY> DATA SECURITY SYSTEM

---

## 6.1. Definitions

## 6.2. References

- P01 – IS Policy
- PR05 - Change Control Procedure
- *<COMPANY> to add further definitions and references*