

<COMPANY>

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

<b>Document Reference</b>	PR04 - Anti-Virus & Malicious Software Procedure
<b>Date</b>	
<b>Document Status</b>	SAMPLE
<b>Version</b>	2.0
<b>Revision History</b>	

## Table of Contents

1.	<b>Purpose</b> .....	3
2.	<b>Scope</b> .....	3
3.	<b>Roles and Responsibilities</b> .....	3
4.	<b>Procedure</b> .....	3
4.1.	<b>Anti-Virus Software Installation</b> .....	3
4.2.	<b>Anti-Virus Software Testing</b> .....	4
5.	<b>Enforcement</b> .....	4
6.	<b>Definitions and References</b> .....	4
6.1.	<b>Definitions</b> .....	4
6.2.	<b>References</b> .....	5

## 1. Purpose

This document details the measures that must be taken by <COMPANY> employees to help achieve effective virus detection and prevention. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, and removable media. 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.

## 2. Scope

This procedure applies to all computers that run the Microsoft ('MS') Windows <COMPANY to define> operating system and are connected to <COMPANY>'s cardholder data environment via a standard network connection or virtual private network connection. The definition of computers includes desktop workstations, laptop computers, handheld computing devices and servers.

## 3. Roles and Responsibilities

<COMPANY>'s [RESPONSIBLE TEAM] - Responsible for executing and implementing this procedure.

<COMPANY> [ROLE NAME] - Responsible for monitoring the implementation of this procedure.

See [P01 – Information Security 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 and servers running the MS Windows operating system, following the vendor installation guide provided with the software.
- The anti-virus software console window provides complete access to the options available.
- The anti-virus software includes the full version of <Name / Version> anti-spyware module, which protects computers from malicious software that is not categorised 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 anti-virus server will conduct a weekly scan of all workstations and servers running the MS Windows <COMPANY to define> operating system on the <COMPANY> cardholder data environment. The Full Scan item scans every file on each computer, can be memory-intensive, take several hours to complete and so is scheduled to run over night or at 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 is performed:

<COMPANY>

Document Name: **PR04-Antivirusmalicioussoftwareprocedure**

Version: **v2.0**

Date Last Updated:

Page 3 of 5

- Full Scan Report Review: <COMPANY>'s [RESPONSIBLE TEAM] review the scan report.
- Full Scan Corrective Action: <COMPANY>'s [RESPONSIBLE TEAM] 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 definition (signature) files and the scan engine version being used.
  - The antivirus server <hostname> is configured to check the vendor's website for updates on an hourly basis. All <COMPANY> servers and workstations are updated from the anti-virus server. The anti-virus server, <hostname>, is located in the <COMPANY> data centre environment.
  - If any machine fails an anti-virus update, the <COMPANY>'s [RESPONSIBLE TEAM] will run a manual update, establish the cause of failure and resolve the issue, and notify the <COMPANY> [ROLE NAME] of actions taken.
  - Scan engine version patches are only installed onto the anti-virus server when a major version change is implemented. This is done manually from the vendor website, and after being successfully tested, is installed automatically onto all other <COMPANY> servers and workstations running the Microsoft Windows <COMPANY to define> operating system.

#### 4.2. Anti-Virus Software Testing

- After installation and as a minimum annually, 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). (<COMPANY> to confirm that this activity is completed).

### 5. Enforcement

Any employee found to have violated this procedure will be subject to <COMPANY> disciplinary procedures, as detailed in the <COMPANY> Staff Handbook.

### 6. Definitions and References

#### 6.1. Definitions

- **IS:** Information Security
- **Payment Card Industry Data Security Standard (PCI DSS):** Currently referenced directly from The PCI Security Standards Council's online resource at <https://www.pcisecuritystandards.org>

- **QSA:** Qualified Security Assessor. A third party assessor that conducts onsite PCI audits for Service Providers and Merchants. The QSA is certified annually by The PCI Security Standards Council.
- **ASV:** Approved Scanning Vendor. A third party assessor that conducts quarterly PCI scans against the external card processing environment. The ASV is certified annually by The PCI Security Standards Council.
- **Schemes.** Credit Card Associated companies that include Visa, MasterCard, Amex, JCB, Diners.
- **Merchant.** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and / or services. Note that a merchant that accepts payment cards as payment for goods and / or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
- **Service Provider.** Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.
- **Acquirer.** Bankcard association member that initiates and maintains relationships with merchants that accept payment cards.
- **Cardholder data:** Full magnetic stripe or the PAN plus any of the following: Cardholder name, Expiration date, Service Code.
- **Cardholder Data Environment:** Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

## 6.2. References

- P01 - Information Security Policy
- PR05 - Change Control Procedure