North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

IT Anti-virus Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29.11.2016
Name of Responsible Officer:	Phill Wade, Head of Technology Management and Operations
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09.01.2018
Review date:	25.05.2018
Target audience:	All NHS South, Central & West CSU staff and Customer organisations

Document Control Sheet

Title	**IT Anti-virus Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Stuart Collier – Information Security Manager
Date Created	03.01.2013
Date Last Updated	14.12.2017

History			
Version	Date	Author(s)	Comments
0.1	03.01.2013	Stuart Collier	Draft
1.0	06.01.2016	Phill Wade	SCW CSU Updates and version reset
1.1	02.08.2016	Arif Gulzar	Updated review date, section 2.2, 4.1 and Appendix A
1.2	22.09.2016	Andy Ferrari	Updated as per feedback from IT Senior Leadership Team
1.2	04.10.2016	Arif Gulzar	Signed off by Information Governance Steering Group
2.0	29.11.2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14.12.2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	**Title and contact**
Catherine Dampney	CIO
Phil Evans	Associate Director of IT Services

Contents

1 Introduction

This document forms part of the NHS South, Central and West Commissioning Support Unit (CSU) Information Security Management System.

This document provides detailed policies that govern the operation and use of software specifically designed to protect NHS South, Central and West CSU connected systems from malicious software.

1.1 The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that:-

- Set out the governance of IT security.
- Provide high level policy statements on the requirements for managing IT security.
- Define the roles and responsibilities for implementing the IT security policy.
- Identify key standards, processes and procedures to support the policy.
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

1.2 Document Purpose

This document provides the detailed Antivirus policy statements that support the overall IT security objectives of the organization as set out in the security statement in the ISMS.

2 Anti-Virus Policy

2.1 Policy Overview

This document contains the Antivirus (AV) policy details including actions to be taken if non-compliance occurs. A definition of the terms 'virus', 'malware' and 'spam' are described as well as the approved AV software and configuration standards in the appendices

2.2 Policy Scope

This policy applies to all employees including temporary staff, sub-contractors, contractors, third parties and Customers.

2.3 Policy Detail

- All workstations, laptops and servers must be running approved antivirus protection which has been configured in accordance with appendix A.
- All removable media must be AV scanned prior to use.
- Users must not accept, or run, software from non-trusted sources.
- Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojans, e-mail bombs, etc) into NHS South, Central and West CSU networks or systems
- Users wishing to use personal equipment to access NHS South, Central and West CSU systems must have suitable anti-virus software installed, maintained and configured. These users must also comply with relevant remote access policies.
- Users must inform the IT Service Desk immediately if a virus is detected on their system.

2.4 Policy Non-Conformance

Any system or workstation found to be without adequate protection as defined by this policy will be removed from the network until adequate protection is implemented.

Any user being found to be wilfully violating the anti-virus policy may be subject to one or more of the following sanctions:

- Removal of any equipment used from the network until adequate protection is implemented
- Revocation of rights to access NHS South, Central and West CSU systems
- Any costs incurred by the IT department to remove the virus may be passed on to the department or organisation responsible for the outbreak.
- Subject to disciplinary action

In the event of a virus outbreak, the IT Team reserves the right to temporarily remove equipment, or disable parts of the network to safeguard other systems.

3 Procedure for suspected infection

If a user suspects the system may be infected, the following actions must be taken

- Inform the IT service desk immediately
- Switch off the machine
- Ensure no-one uses the machine
- Be prepared to inform IT of any actions taken which may have caused the infection.

The IT Team will:

- Check the infected PC and any media
- Rebuild the PC if the infection is severe (e.g. Conficker, Cryptolocker)
- Check any servers that may have been accessed from the infected system
- Attempt to determine the source of the infection
- Ensure the incident is logged.

4 Review of Policy

4.1 Review Timetable

As part of the Information Security Management System, this policy will be reviewed on a continual basis by the Cyber Security Manager. This policy will also be reviewed as part of the annual review of the ISMS.

Appendix A **AntiVirus Standard Products**

Approved Software Products

Product	Protecting
McAfee VirusScan Enterprise LANDesk Management Suite	Windows Servers Windows Workstations
McAfee DLP Endpoint	Windows Servers Windows Workstations
Sophos Endpoint Security and Control	Windows Servers Windows Laptops Windows Workstations
McAfee Endpoint Protection Microsoft BitLocker	Windows Laptops
Kaspersky Endpoint Security 10	Windows Servers Windows Laptops Windows Workstations

Configuration Standards

Approved AntiVirus software should be installed and configured to the following standards on all applicable desktop and server equipment:

- All Antivirus configuration settings will be locked down to prohibit unauthorised users from disabling the software or altering the standard configuration
- Antivirus software on laptops and desktops will periodically check (at least daily) for updates to the AntiVirus engine and the DAT (pattern/signature) file and will automatically apply.
- Antivirus software on servers and gateways will check for updates on a (minimum) daily basis.
- Antivirus will be automatically enabled at all times when the system is in use with the following exceptions:
    - When software upgrades dictate disablement
    - To facilitate problem diagnosis.

Appendix B

The following ISO27001 controls are relevant to this policy

A.10.4.1 Controls against malicious code
A.10.4.2 Controls against mobile code

Appendix C – Glossary of terms

Adware	Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.
Antivirus Software	A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term *antimalware* is preferred because it covers more threats.
Browser Hijacker	A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.
Dat Files	Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.
Keylogger	Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.
Malware	A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.
Phishing	A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.
Ransomware	Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.
Spam	An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information. Email messages are not considered spam if a user has signed up to receive them.
Spyware	Spyware spies on a user's computer. Spyware can capture information like web browsing habits, email messages, usernames and passwords, and credit card information. Just like viruses, spyware can be installed on a computer through an email attachment containing malicious software.
Trojan	Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.