South, Central and West
Commissioning Support Unit

Anti-Virus Policy
Version 3

South, Central and West Commissioning Support Unit
July 2018

DOCUMENT CONTROL

Document Name	Version	Status	Author
Anti-Virus Policy	*3.0*	*Final*	*Cyber Security Manager*
Document objectives:	*This policy is designed to give guidance and direction to staff on minimising the risk of a virus/malware infection, and what to do if they are encountered.*		
Target audience:	*All staff*		
Committee/Group Consulted:	*SCW Information Governance Steering Group*		
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*		
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages*		
Approved and ratified by:	*SCW Information Governance Steering Group SCW Corporate Governance Assurance Group*	*Date: 24 July 2018*	
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*	
Date issued:	*24 July 2018*		
Review date:	***July 2019***		
Author:	*Cyber Security Manager*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
03/01/2013	Stuart Collier	0.1		Draft
06/01/2016	Phill Wade	1.0		SCW CSU Updates and version reset
02/08/2016	Arif Gulzar	1.1		Updated review date, section 2.2, 4.1 and Appendix A
22.09.2016	Andy Ferrari	1.2		Updated as per feedback from IT Senior Leadership Team

04/10/2016	Arif Gulzar	1.2		Signed off by Information Governance Steering Group
29/11/2016	Arif Gulzar	2.0		Version reset after ratification from Corporate Governance Assurance Group
14/12/2017	Arif Gulzar	2.1		Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group
18/05/2018	Arif Gulzar	2.2	All	Updated policy template with corporate branding. Updated section 1.2, 2.2 & 2.3 Added section 3 for Exceptions Added section 4 for Monitoring & Compliance
21/05/2018	Arif Gulzar	2.3		Policy reviewed and approved by IT senior leadership team.
24/07/2018	Arif Gulzar	3.0		Version changed after CGAG ratification

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V2.2 21/05/18
Andy Ferrari	Associate Director of IT Strategy and Planning	V2.2 21/05/18
Cathy Jukes	Associate Director of IT Projects and Programmes	V2.2 21/05/18
Michael Knight	Associate Director of Technology Management and Architecture	V2.2 21/05/18
David Walch	Head of IT Service Delivery	V2.2 21/05/18
Stephanie Wilson	Head of Service Development and Support	V2.2 21/05/18

TABLE OF CONTENTS

1 INTRODUCTION

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

This document provides detailed policies that govern the operation and use of software specifically designed to protect SCW 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.

This document provides the detailed antivirus policy statements that support the overall IT security objectives of the organisation as set out in the security statement in the ISMS. Effective implementation of this policy will limit the exposure and effect of viruses or malware threats to the systems supported and managed by SCW.

2 SCOPE OF 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 standards in the appendices

2.2. POLICY SCOPE

This policy aims to set out anti-virus policy within SCW IT services. This policy applies to all SCW staff authorised to use/access IT systems and communications networks whether they are employed directly by SCW, customer organisations, contractors, NHS Professionals, bank staff, voluntary organisations or suppliers granted access for support purposes.

2.3. POLICY DETAIL

Configuration Standards

2.3.1. Approved Anti-virus software MUST be correctly installed and configured on all supported endpoint and servers across SCW network to the following configuration standards. See the list of approved software in appendix A.

2.3.2. Anti-virus software MUST be kept up to date including the definitions files.

2.3.3. Anti-virus software updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 60 minutes daily.

2.3.4. Virus and malware signature updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for signature updates every 10 minutes daily. All the endpoints must be configured with the secondary anti-virus update server so if a device is not checked in on the corporate network then updates will be installed from the secondary server.

2.3.5. Anti-virus software MUST be configured for real time scanning and regular scheduled scans.

2.3.6. On-access scanning MUST be configured within Anti-virus software for removable media and websites.

2.3.7. Anti-virus server MUST be monitored on a daily basis by a nominated staff within Technology Management and Architecture team for virus alerts and any issues which cannot be resolved remotely via centralised management console must be escalated to the IT Service Desk where an incident will be raised and a technician assigned to immediately investigate.

2.3.8. In the event of a virus infection which infects multiple devices (more than 3 devices) at the same time. A root cause analysis report should be completed by the technician for SCW Cyber Security Manager

2.3.9. Monthly Anti-Virus compliance reports MUST be provided to the SCW Cyber Security Manager, Locality Manager and IT Strategy & Planning Team by the third working day of the month. In the event that systems are found to be non-compliant a report including suggested remediation will be created by the Technology Management and Architecture team which will be provided to SCW IT Senior Leadership Team (SLT)

2.3.10. Tamper protection MUST be enabled to prevent end users or malware altering the anti-virus software's configuration or disabling the protection

User Responsibilities

2.3.11. All IT equipment and removable media MUST be scanned for viruses and malware before being introduced or prior use on the corporate network, system or device

2.3.12. Users MUST not accept, or run, software from non-trusted sources

2.3.13. 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 corporate network(s) or system(s)

2.3.14. Users MUST inform the IT Service Desk immediately if a virus is detected on their system

2.3.15. IT system(s) infected with a malware/virus that the anti-virus software has not been able to deal with MUST be disconnected/quarantined from the corporate network until virus free

3 EXCEPTIONS

3.1. Exceptions to the anti-virus policy require a formal documented risk assessment including steps taken to mitigate the risk and formal approval from the Associate Director of TMA. Once approved exceptions will be implemented via the SCW Change and Configuration Management process.

3.2. Any server or workstation that do not comply with policy must have an approved exception recorded in the Anti-virus exceptions file detailing the reason for the exception and the steps taken to mitigate the risk.

3.3. Systems will only have exception to the policy if scheduled updates or patches are deemed likely to cause major disruption to the system, resident software or service functionality or to facilitate problem diagnosis. All systems recorded within the Anti-virus exceptions file must be reviewed on a quarterly basis by the TMA team and the risk will be re-evaluated.

4. MONITORING AND COMPLIANCE

Anti-virus compliance level refers to the percentage of servers, workstations and laptops that have been successfully protected by an up to date Anti- virus product against virus or malware threats.

4.1. SCW IT services will endeavour to achieve 100% compliance for all the end points under its management. For monitoring and compliance assessment the following levels must be maintained at all times

4.2. **100% of all servers** must be protected with up to date anti-virus software and virus signatures installed no more than 2 days of signatures being released by the vendor

4.3. **97% of all Desktops/laptops** must be compliant with up to date anti-virus software and virus signatures installed within 2 days of the release

5. 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 SCW systems

Version Number: 3.0	Issue/approval date: 24 July 2018
Status: Final	Next review date: July 2019

- 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.

6. 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. Dridex, Ransomware)
- 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

7. REVIEW OF POLICY

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 Antivirus Software Products

Trend Micro Endpoint security including IDS/IPS
Sophos Endpoint Protection
McAfee VirusScan Enterprise
Windows Advanced Threat Protection
Symantec Endpoint Protection
Kaspersky Endpoint Security 10
LANDesk Management Suite
Panda Adaptive Defense 360
Malwarebytes Endpoint Protection/Security

APPENDIX B – ISO CONTROLS

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.

APPENDIX D - EQUALITY IMPACT ASSESSMENT

For IT Anti-virus Policy

1.	Title of policy/ programme/ framework being analysed IT Anti-virus Policy.
2.	Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives? To provide a framework of guidance to NHS South, Central and West CSU (SCW) staff (as defined in the scope) regarding the security of Personal and Sensitive Data in both paper and electronic form.
3.	Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers Staff.
4.	What evidence do you have of the potential impact (positive and negative)? None expected.
4.1	Disability (Consider attitudinal, physical and social barriers) No impact
4.2	Sex (Impact on men and women, potential link to carers below) No impact
4.3	Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences). No impact
4.4	Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare). No impact
4.5	Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment) No impact
4.6	Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people). No impact
4.7	Religion or belief (Consider impact on people with different religions, beliefs or no belief) No impact
4.8	Marriage and Civil Partnership No impact
4.9	Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities). No impact
4.10	Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation). No impact
4.11	Additional significant evidence (See Guidance Note)

Give details of any evidence on other groups experiencing disadvantage and barriers to access due to: • socio-economic status • location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5. Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.
Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 23 July 2018
Name and signature of responsible Director Simon Sturgeon, Director of IT Services
Date analysis was approved by responsible Director 23 July 2018

End of Policy Document