Information Security Policy
Virus and Malware Protection

Author:	**Information Security Manager**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Quality Assurance and Improvement Committee**
Governance or Assurance Committee	**Information Governance Committee**
Implementation Date:	**March 2017**
Version Number:	**2.6.5**
Last Review Date:	**Aug 2021**
Review Date:	**Aug 2024**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager, eHealth
Consultation Process / Stakeholders:	• Donald Wilson, General Manager, eHealth & Senior Information Risk Owner (SIRO) • Information Governance Committee members
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Oct 2016	A Ashforth	First Draft : New policy identified as a gap after review using SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5
Jan 2017	A Ashforth	Resolve typos	2.5.1
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.2
April 2018	A Ashforth	Reviewed in line with General Data Protection Regulation (GDPR)	2.6
June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.1
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.2
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.3
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.4
June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section Amend start of section 4.1.1 to switch off computer as well as disconnect from the network, as laptops will use Wi-Fi usually instead of hard wired connection. Amend section 4.1.1 – remove ‘Staff should ensure that the virus checking software is up to date’ as most staff will not know how to check this. Amend section 4.1.1 - Replace 'All staff	2.6.5

		should be aware that malware can be brought into NHSL accidentally by staff clicking on a web link in an email or email attachment or simply when accessing the Internet, and this may not be blocked by the NHS Lanarkshire Anti-Virus management platform.' with 'Staff should take care when accessing the Internet and be aware that web links in emails could be used to direct staff to malicious sites.'	

1. Introduction

This policy relates to virus and malware* protection and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

To ensure that INFORMATION SECURITY is maintained

- Ensure that confidentiality and integrity of personal and sensitive information is maintained
- Ensure that information is available to ***authorised*** users
- Ensure that information is not disclosed to ***unauthorised*** people
- To prevent ***destruction*** of information

This document forms the NHS Lanarkshire Virus and Malware Protection Policy, in support of the NHS Lanarkshire Information Security Policy. This document is part of the Information Security Management System (ISMS) for NHS Lanarkshire and describes the measures the organisation takes to control mobile and malicious code i.e. viruses, that may potentially infiltrate into the organisation.

Compliance with it will help protect NHS Lanarkshire from malware and provide the means to minimise disruption and business impact should preventative measures fail.

This policy forms part of eHealth Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This policy has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the policy will be reviewed to meet future changes to this standard.

This policy has been written to comply with current legislation and the policy will be updated appropriately to suit new and/or modified legislation. The references appendix will be updated to reflect this legislation.

***Malware**' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

3. Scope

3.1 Who is the Policy intended to Affect?

This policy is for eHealth staff for all systems managed by eHealth.
In the interests of clarity all references to 'staff' includes all staff within NHS Lanarkshire and all staff who are employed, engaged or partners within each GP practice (contracted to NHS Lanarkshire).

3.2 Who are the Stakeholders

All staff.

NHS Lanarkshire take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process your information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk or ask a member of staff for a copy of our Data Protection Notice.

4. Principal Content

4.1. RESPONSIBILITY

4.1.1 All staff

Anyone who believes or suspects that their computer has been infected with a virus is to immediately shut the computer down and remove it from the network by disconnecting the Ethernet cable at the back of the computer, and inform the IT Service Desk as soon as possible.

Virus infected computers are to remain shut down and isolated from the network until you are told by a member of the eHealth IT staff, that they can be reconnected. The person who was using the computer the time it became, or was suspected of becoming infected is to clearly label the computer that it is virus contaminated and must not be reconnected to the network without the authority of the eHealth IT Department.

Any removable media being used on the computer at the time of the suspected contamination, or immediately prior, is to be handed to the eHealth IT support staff, for investigation.

Staff should take care when accessing the Internet and be aware that web links in emails could be used to direct staff to malicious sites. Appendix 2 provides tips to deter malware attacks when using Email and Internet.

4.1.2 eHealth Department

The NHS Lanarkshire eHealth Department will deploy, operate and maintain up to date effective anti-virus software on all computer systems that could be attacked by malicious software.

All networked PCs/Laptops will be updated with the latest applicable virus definition when it becomes available.

Only authorised eHealth staff may deploy anti-virus software on to NHS Lanarkshire computers.

eHealth staff who discover virus incident must inform the IT Service Desk. The eHealth Information Security Manager will be informed that an incident has occurred.

4.1.3 Line Managers

It is the responsibility of the Line Manager to ensure this policy is deployed within their area of responsibility.

4.1.4 Third Parties

All third party servers which are either not connected to NHS Lanarkshire domains or not managed by an NHS Lanarkshire Anti-Virus management platform must have appropriate virus and malware protection in place.

All third party appliances must be checked for viruses before connecting to the NHS Lanarkshire computer network.

4.2 OPERATIONAL SYSTEMS

NHS Lanarkshire will use anti-virus software products to protect desktop, laptop and tablet computers, servers, and any other information systems.

Automatic anti-virus software updates and scanning configuration will be provided centrally.

4.2.1 Malicious Code

Malicious code is defined as a computer virus, network worm, Trojan horse or other malware including ransom ware that when ran may damage the confidentiality, integrity or availability of an information processing system.

4.2.2 Mobile Code

Mobile code is defined as software code that transfers from one computer to another and then executes automatically, performing a specific function with little or no user interaction.

Whilst many websites may use mobile code, such as Java or ActiveX, for legitimate purposes, the same technology can be used for clandestine means, and therefore, where

mobile code is allowed, specific technical controls must be utilised to ensure the integrity of information systems.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager, eHealth
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance Committee

6. Resource Implications

No resource implications

7. Communication Plan

This policy will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

8. Quality Improvement – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

9. Equality and Diversity Impact Assessment

This policy meets NHS Lanarkshire's EDIA [X] (tick box)

10. Summary of Frequently Asked Questions (FAQs)

N/A

11. References Appendix 1

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this policy are:

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- Scottish Health Competent Authority - NCSC Cyber Assurance Framework
- Scottish Health Competent Authority - Information Security Policy Framework (ISPF) 2018
- Scottish Government Public Sector Cyber Resilience Framework
- Scottish Government Public Sector Action Plan 2017-18
- CEL 25 (2012) NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- MEL 2000 (17) Data Protection Act 1998

- NHSL Risk Management Strategy 2016
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012
- SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

11. Tips to deter Malware Attacks when using Email and Internet – Appendix 2

The emails usually have a document attached which may have a macro embedded within it. Macros are disabled by default in the Microsoft Office applications to reduce the risk that macros are run automatically should the document be opened. The macros in the documents have been set up to download and install malware.

Alternatively, the attached document in the email may look like an excel spread sheet and contain an excel button labelled in such a way to entice staff to click on the button, for example, “display the contents of the document”. This is to download and install malware.

Top tips

Follow the tips below for all email you receive and websites you access:

- **DO NOT** click, download, open or execute any attachments or links from emails that are not expected and to the best of your (the recipients) ability verified as legitimate.
- **DO NOT** follow the advice given in an email to enable editing and/or enable macros to see the content.
- **DO NOT** follow the advice given in the preview of the attachment to enable editing and/or to click on the button to see the contents of the document.
- **DELETE** emails that you think are not legitimate.
- **DO NOT** download or install additional software/browser plug-ins from un-trusted web sites.