Information Security Policy
Secure Use of Remote Access

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:	**September 2010**
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, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance Committee members
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Mar 2006	A Ashforth	Revised in view of new policy template	1.0
Mar 2007	A Ashforth	Revised in view of new policy template	1.0
Sept 2010	A Ashforth	Revised in view of new policy template	2.0
May 2013	A Ashforth	Revised in view of comments	2.2
May 2013	A Ashforth & C Tannahill	Revised in view of comments	2.3
Aug 2014	A Ashforth & C Tannahill	Minor change - Reference appendix updated Minor change - some rewording throughout	2.4
Aug 2015	A Ashforth	Minor change - Reference appendix	2.5
Oct 2016	A Ashforth	Reviewed in line with SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	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	2.6.5

		GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section Amend section 4 – 'Supported Technology' that only laptops provided by NHSL will be supported. Also, add 'iPads may also be enabled for access to certain systems such as Morse.' Amend section 4 – 'Eligible Staff' that the request should be made through the IT Service Desk. Amend section 4 – 'Policy and Appropriate Use' item 5 – remove reference to NHSmail and provide a link to the email acceptable usage policy. Amend 'Policy and Appropriate Use' section, bottom of page 7 – add 'Staff must ensure they comply with the Home Working IS Policy.'	

1. Introduction

This policy relates to Remote Access 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

The purpose of this policy is to define the standards, procedures and restrictions that staffs of the NHS Lanarkshire (NHSL) IT remote access service must adhere to in order to connect and use this service appropriately.

Advise staff of their obligations to maintain information confidentiality, integrity, and availability.

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.

3. Scope

3.1 Who is the Policy intended to Affect?

This policy is intended for all NHS Lanarkshire staff to maintain information security. 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).

This policy also applies to all staff, external IT contractors, suppliers and agencies who are provided by the NHSL eHealth Department with access to the NHSL remote access portal and the IT services made available from this portal.

All remote access transactions using this service are covered by this policy.

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

Supported Technology

Access to the secure remote access service can be provided to staff using an NHSL provided laptop providing a working broadband connection is in place. iPads may also be enabled for access to certain systems such as Morse.

The NHSL eHealth Department cannot provide installation support for any user of privately owned ISP connections (wired or wireless) to connect to the NHSL secure remote access portal. Staff who require this help need to consult their ISP provider for this assistance.

Eligible Staff

Staff may request access to the secure remote access service through the IT Service Desk.

The IT Service Desk must receive approval from the Line Manager of the requesting employee (an email approval is acceptable) before the request can be assigned to arrange installation.

Policy and Appropriate Use

It is imperative that the remote access service is used by staff appropriately, responsibly and ethically at all times. The following rules of use must be adhered to by staff at all times:

1. Staff need to take care when using the secure remote access service as non-NHS access to systems will be direct to the Internet via an Internet Service Provider (ISP) or NHSL provided ISP (GPRS/3G/4G wireless broadband card users).

2. Staff will follow the NHSL secure remote access user guide before attempting to access the secure remote access portal for the first time.

3. Staff will take all reasonable precautions to prevent unauthorized access to their computer.

4. Staff will only use the authentication and access solutions provided by the NHSL eHealth Department to make remote connections to the NHS secure remote access service.

5. Staff provided with NHSL secure remote access must never use non-NHS e-mail accounts (e.g. Hotmail, Yahoo, Gmail etc.) to conduct any NHSL business. Staff should use the NHS Lanarkshire email system. For further details on email acceptable use please refer to the Email Acceptable Usage Policy.

6. All suspected or actual unauthorized access and/or disclosure of NHSL resources, databases, and networks must be reported immediately by the employee to their Line Manager and the NHSL IT Service Desk.

7. Staff agree to and accept that their remote access connection to the NHSL network will be monitored to record dates, times, duration of access, etc., in order to identify any unusual usage patterns or other suspicious activity. This will be undertaken in order to identify accounts/computers that may have been compromised and represent a security risk to NHSL.

8. Any employee issued by the NHSL eHealth Department with a wireless GPRS/3G/4G broadband device, must use this device only on the NHSL computer they have been issued with.

Staff must ensure they comply with the Home Working IS Policy.

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