Information Security Policy
Secure Use of Application Systems

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 2012	A Ashforth	Revised in view of comments	2.1
July 2013	A Ashforth	Revised in view of comments	2.2
May 2014	A Ashforth & C Tannahill	Revised in view of comments	2.3
Aug 2014	A Ashforth & C Tannahill	Main change - rewording throughout sect. 4 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
Oct 2016	A Ashforth	New section 4.3 – Use of Privileged Utility Programs	2.5.2
Dec 2016	A Ashforth	Small change to pt 4.3.2	2.5.3
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.4
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	2.6.5

1. Introduction

This policy relates to Secure Use of Application Systems and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

2.1 To ensure that INFORMATION SECURITY is maintained

2.1.1 Ensure that confidentiality and integrity of personal and sensitive information is maintained

2.1.2 Ensure that information is available to *authorised* users

2.1.3 Ensure that information is not disclosed to *unauthorised* people

2.1.4 To prevent *destruction* of information

2.2 The purpose of this policy is to provide guidelines for the secure use of computer systems/applications in the NHS Lanarkshire (NHSL). A computer system/application can be defined as a software system on a computer that is typically used within a department to support the regular business or clinical activities of that department. Hence a computer application system, on a PC, used by a cash office to manage patient monies can be thought of in this context. This is distinct from the generalised use of PCs and software such as using a computer to do word processing. A computer system/application can be thought of as a dedicated software system on a computer that performs functions for a whole department or area.

2.3 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).

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 Application System

4.1.1 An application is a computer system or software program, authorised and provided by your eHealth department that is either pre-installed or specifically required as part of your job role.

4.2 Application Security

4.2.1 Application Security refers to the controls that are built into a software application to ensure that the confidentiality, integrity and availability of a system and its related data can be maintained. These are the three basic principles for information security.

4.2.2 Application security controls are designed to ensure that:-

4.2.2.1 Only authorised staff of an application will have access to it; typically there will be a systems administrator who will allocate user credentials on request, following a formalised approval procedure.

4.2.2.2 The user is identified by their individual username and password.

4.2.2.3 The level of access permitted is determined by job role.

4.3 Use of Privileged Utility Programs

Most computer installations have one or more utility programs that might be capable of overriding system and application controls.

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

The following guidelines for the use of utility programs that might be capable of overriding system and application controls should be considered.

4.3.1 Use of identification, authentication and authorization procedures for utility programs.

4.3.2 Segregation of access to utility programs from general applications software.

4.3.3 Limitation of the use of utility programs to the minimum practical number of trusted, authorized staff

4.3.4 Authorization for ad hoc use of utility programs.

4.3.5 Limitation of the availability of utility programs e.g. for the duration of an authorized change.

4.3.6 Logging of all use of utility programs.

4.3.7 Defining and documenting of authorization levels for utility programs.

4.3.8 Removal or disabling of all unnecessary utility programs.

4.3.9 Not making utility programs available to staff who have access to applications on systems where segregation of duties is required.

4.4 Access to Systems

4.4.1 Access to applications is managed by authorisation, approval and creation of a user account by the system administrator.

4.4.2 Staff will be provided with individual user account and password and receive training.

4.4.3 The line manager is responsible for informing the eHealth department of any staff member who no longer requires access to IT systems; this is to ensure their account is disabled.

4.4.4 There may be temporary user accounts for operational reasons such as in A&E who have a super user who can create temporary access accounts for locums.

4.4.5 An audit log is maintained on all IT systems. An example of a system audit log, would contain a user(s) login, date, time of access and activity performed, this includes viewing of records. Audit logs are monitored and reviewed regularly.

4.5 Security of Information in Computer Systems

4.5.1 Patients and staff have a right to expect that information about them will be treated as confidential. Staff may have access to privileged information and have a duty to maintain the security and confidentiality of the data that are held by NHSL.

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