Information Security Policy
User Access Rights

Author(s):	**Information Security Manager** **Head of Digital Transformation**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Quality Assurance and Improvement Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**June 2017**
Version Number:	**2.6.6**
Last Review Date:	**Dec 2023**
Review Date:	**Dec 2026**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager • Barry McAlister, Head of Digital Transformation
Consultation Process / Stakeholders:	• Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
March 2017	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
June 2017	B. McAlister	Additions 4.5, 4.6, 4.7, 4.8	2.5.1
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
Dec 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. 4.3 Review of User Access Rights - Movers & Leavers - added 'When a member of staff leaves their current role their line manager must raise a ServiceDesk call, specifying which systems should be removed for this user.' 4.6 Disabling of User Accounts – Leavers - added 'When a member of staff leaves	2.6.6

		their current role their line manager must raise a ServiceDesk call, specifying which systems should be removed for this user.' References Appendix 1 – updated.	

1. Introduction

This policy relates to user access rights and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

The aim of this policy is to provide a consistent and robust electronic access control framework to ensure the availability of information and telecommunication services within NHS Lanarkshire.

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, and procedures for user access rights in order maintain information confidentiality, integrity, and availability.

It details existing policy and controls surrounding access control to the Digital Infrastructure, and requires system manager to regularly review users' (staff) access rights.

This policy forms part of the 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

The Digital department uses user access rights and other security measures to protect the confidentiality, integrity, and availability of any information processed by computers and communications systems, and to assure that individuals will be held accountable for information that is accessed and processed.

In pursuit of these security objectives, the Digital department maintains the authority for the following actions:

- regular review of users' access rights after any staff changes, such as promotion, demotion or termination of employment (inspect and adjust or remove);
- review user access rights when moving from one role to another within the same organization (inspect and adjust);
- authorizations for privileged access rights will be reviewed at more frequent intervals (inspect);
- privilege allocations will be checked at regular intervals to ensure that unauthorized privileges have not been obtained (inspect);
- changes to privileged accounts will be logged for periodic review (record).

The Digital department imposes the following policies in regard to access control:

- Digital will not share information systems or allow unsupervised access to its systems by third party organisations unless organization via change management;
- Digital takes all reasonable steps to prevent unauthorised access to its systems, both from inside and outside NHS Lanarkshire;
- System access is provided to staff based upon the needs of their jobs and their job role;
- Digital provides function-specific storage where individuals may store data, which is personal and privy to their job role, as well as areas where they may share information within defined groups;
- Individual's access to facilities and data is determined and granted by the individual's Head of Department;
- The facilities which any department has rights of access to are in turn laid down according to the department's function within the organization;

4.1 User Registration

User registration at NHS Lanarkshire ensures the following:

- using unique user IDs so that staff can be linked to and made responsible for their actions;
- checking that the user has authorisation from their Head of Department to use the information system or service. Separate approval for access rights from management may also be appropriate;
- checking that the level of access granted is appropriate to the business purpose and is consistent with the security policy, e.g. it does not compromise segregation of duties;

- ensuring service providers do not provide access until authorisation procedures have been completed;
- maintaining a formal record of all persons registered to use the service;
- periodically checking for, and removing, redundant user IDs and accounts;
- ensuring that redundant user IDs are not issued to other staff;

4.2 Privilege Management

The privileges associated with each system product, e.g. operating system, database management system and each application, and the categories of staff to which they need to be allocated have been identified.

Privileges are allocated to individuals on a need-to-use basis and on an event-by-event basis, i.e. the minimum requirement for their functional role only when needed.

An authorization process and a record of all privileges allocated are maintained. Privileges should not be granted until the authorization process is complete.

The allocation of special system privileges is appropriately authorized within NHS Lanarkshire and restricted to as few people as possible.

4.3 Review of User Access Rights - Movers & Leavers

Heads of Department shall ensure the immediate removal of access rights of staff who have changed jobs or left NHS Lanarkshire i.e. complete the mover/leaver form and return to HR & forward it to the Digital Department for implementation.

When a member of staff leaves their current role their line manager must raise a ServiceDesk call, specifying which systems should be removed for this user.

An individual's Head of Department shall ensure that if their job role changes they do not have more rights than is necessary for them to carry out their responsibilities.

4.4 Digital Department

Access rights are reviewed on change of job role.

Only authorised members of the Digital staff are given admin rights to the systems they are expected to manage and depending on their job role.

4.5 Departmental System Administrators

Systems that are managed by departments other than Digital will be managed in line with this policy. It is the responsibility of the Head of Department to ensure that these processes and controls are in place.

4.6 Disabling of User Accounts – Leavers

Digital has an agreed user de-provisioning process. The payroll department provides Digital with a monthly file of leaver and changes. Digital will use this list to disable the relevant accounts.

When a member of staff leaves their current role their line manager must raise a ServiceDesk call, specifying which systems should be removed for this user.

If a user has changed role and their account was disabled, Digital will check any changes to access groups the staff member requires for their new role before re-enabling their account.

In addition, a standard process will automatically disable accounts that have not been accessed for more than 45 days.

4.7 Deletion of User Accounts

Following the disabling process for accounts, a process to completely remove and delete accounts will take effect.

Once a period of 18 months has passed any accounts that were previously disabled will be permanently removed.

4.8 Management of User Accounts of Suspended Staff

Line Managers must ensure that they make the Service Desk aware when a member of staff is suspended.

Digital will disable the user account as soon as this information is received.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager Head of Digital Transformation
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance 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)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- 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 Framework
- 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