Information Security Policy
Secure Use of Passwords

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 and Cyber Assurance Committee**
Implementation Date:	**September 2010**
Version Number:	**2.7**
Last Review Date:	**Oct 2023**
Review Date:	**Nov 2026**

CONTENTS

i) Consultation and Distribution Record
ii) Change Record

1. INTRODUCTION

2. AIM, PURPOSE AND OUTCOMES

3. SCOPE
   3.1 Who is the Policy Intended to Benefit or Affect
   3.2 Who are the Stakeholders

4. PRINCIPAL CONTENT

5. ROLES AND RESPONSIBILITIES

6. RESOURCE IMPLICATIONS

7. COMMUNICATION PLAN

8. QUALITY IMPROVEMENT – MONITORING AND REVIEW

9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

10. SUMMARY OF POLICY / FAQS

11. REFERENCES – APPENDIX 1

12. SUMMARY OF GOOD PASSWORD PRACTICE – APPENDIX 2

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager
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.**
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
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 - Insertion of new sub-section – Single Sign On Minor change - Reference appendix updated Minor change - some rewording throughout	2.4
Aug 2015	A Ashforth	Minor change - Reference appendix	2.5
Aug 2016	A Ashforth	Minor change – Update to describe password complexity in General section and Appendix 2	2.5.1
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)	2.5.2
Nov 2016	A Ashforth	Minor change – Include references to and section on “Third party suppliers” within policy principles wording.	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
May 2018	A Ashforth	Change to Principle Content – General section – ‘Passwords must consist of a minimum of 8 characters’	2.6.1

June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.2
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.3
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.4
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.5
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. 4. General - new last para - 'Temporary passwords have a forced change when the account is first logged into after being reset by eHealth.' 4. New sub-section 'Administrative and Privileged User Accounts' - 'NHSL are working towards secondary authentication for all administrative and privileged user accounts. Default passwords on all new systems must be changed as part of the installation and commission phase.'	2.6.6
Oct 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. Major update to policy to support longer passwords that change less frequently in line with NCSC guidance using three random words and removing the need for password complexity.	2.7

1. Introduction

This policy relates to Secure Use of Passwords 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

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

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).

This policy also applies to Third Party Suppliers who support NHS Lanarkshire Digital assets.

3.2 Who are the Stakeholders

All staff and Third Party Suppliers.

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

This policy provides practical advice on the use of passwords for access to computer systems. Appendix 2 provides a summary of good practice in respect of passwords.

General

Each member of staff must have his/her individual user account and password. For the most effective security, staff should have self-selected individual passwords that conform to NHS Scotland password standards.

When someone leaves, his/her password and user account must be disabled as soon as possible.

Passwords must not normally be written down. It is not uncommon for password protection to be defeated by a user writing the password down on a piece of paper kept close to a computer.

Passwords must not be displayed on screens as they are entered. Computers should be physically positioned such that they are protected against accidental disclosure of passwords. Keyboards and screens should be positioned such that only the user can view password entry.

Staff should not disclose their passwords to any other person, even Digital staff.

Where possible passwords should not relate to the system being accessed i.e. they must not be the same as the service or system being assessed, e.g. “TrakCare”.

Passwords must not relate to the user. Many staff will opt for passwords that they find particularly easy to remember. Often the password chosen has strong associations with either the system being accessed or the background of the user and can be guessed by potential intruders.

Temporary passwords have a forced change when the account is first logged into after being reset by Digital.

Passwords must always be changed immediately on suspicion of any compromise.

Password Rules

National Cyber Security Centre (NCSC) have updated their advice to organisations and individuals to use longer passwords and change them less frequently. This is to significantly reduce the risk of a password being guessed quickly, as shorter passwords are much easier and quicker to attack, and with a longer password there is less need to change it as regularly.

NCSC have advice on longer passwords using three random words.

Password configuration enforced for all user accounts is as follows:

- Minimum password length **12** characters
- Users are prompted to change their password at first login and 30 days prior to the existing password expiring
- Excluded word list
    - No first names
    - No names of seasons
    - No names of month
    - No common computer terms
- Maximum password age **365** days
- Re-use of recent passwords is not allowed

Single Sign On

All staff will be using Single Sign-On (SSO), this allows staff to login into a PC with their own unique network Username and Password and then be automatically logged into all their key applications.

The key benefit of SSO is to increase front-line efficiency by enabling staff to legitimately access several applications without the need to remember several passwords and log into each of them separately.

If you lock your desktop or laptop and do not return within the 4 hours, your account will be logged out and any unsaved work may be lost. Staff should ensure that all work is routinely saved. This is to improve device performance and reduce the frequency of locked account issues.

It is essential that staff comply with the password policy, and this includes good logging in/out procedures.

If staff forget their password, they can use SSO to do self-service password recovery.

Generic Accounts

The password policy for generic accounts is the same as user accounts except the password never changes, however additional mitigation should be applied such that the generic account should only have login rights on specific workstations with limited rights.

No generic account can be used for access to clinical or corporate systems unless an agreed process is in place to manage this account such that only one user will use it at any one time and the user can be identified e.g. locum account for emergency use out of hours:

- Any request for a generic account to allow access to clinical applications for Locum staff out of hours must be managed by the service requestor.
- The service must record details of Locum user using account for specific dates and times.
- The account will have logon hours set depending on the requirements of the service.
- A request should be logged to change the password for this generic user account for a new user.
- Any use of account out with agreed requirements can result in account being withdrawn.
- Internet access is not available via using account.

The user department must get agreement from the system owner before using a generic user account for access to clinical or corporate systems.

Administrative and Privileged User Accounts

NHSL are working towards secondary authentication such as Multi Factor Authentication (MFA) for all administrative and privileged user accounts. Default passwords on all new systems must be changed as part of the installation and commission phase.

The enforced policy in Active Directory for admin and privileged accounts is similar to normal user accounts with the following differences:

- Admin (workstation/server) – minimum 15 characters, change every 60 days
- Service and remote access for suppliers – minimum 25 characters and set to never expire (other mitigations in place for these accounts such as privilege access management solution and two factor authentication)
- Domain admin - minimum 25 characters, change every 60 days

Third Party Suppliers

All usernames and passwords managed by third parties must comply with this policy.

NHS Lanarkshire is required to maintain an up-to-date database of all usernames and passwords for all Digital assets maintained and managed by Third Party Suppliers. The Information Security Manager will be the custodian of the password database.

The creation, modification and deletion of usernames and/or passwords on Digital assets managed by Third Party Suppliers is subject to NHS Lanarkshire's Digital Change Control Policy.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager
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 Strategy

- 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

12. Appendix 2 – Summary of Good Password Practice

When choosing a password consider:

Excluded Word List

- No First Names – e.g. Jenny or Jamie
- No Seasons – e.g. Summer or Winter
- No Months – e.g. January or May
- No Common Computer Terms – e.g. Password

Secure Password Tips

- Try using 3 Random Words
- Example – OneLoanBikes or TreeBearTruck
- Try Mixing It Up
- Example – LOSTmapsSEek

Keep It Safe

Keep It Secret

Keep It Secure

Any user with allocated an NHSL user account must:

- Be responsible for the security and confidentiality of their password(s)
- **Do not** tell anyone else his or her password
- Be aware of the guidance relating to passwords
- **Do not** write down passwords
- Ensure that when entering a password, the entry cannot be seen by anyone else
- Choose a password carefully
- **Do not** choose a password that relates directly to the system intended to be accessed
- Seek advice from the Service Desk if you forget your password
- **If you can,** change your password immediately if you suspect it has been compromised or alternatively contact the Service Desk for assistance

If you suspect your password has been used by others contact the Service Desk so that the incident can be investigated