## Information Security Policy
### Secure Use of Passwords

<table>
<thead>
<tr>
<th><strong>Author:</strong></th>
<th>Information Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsible Lead Executive Director:</strong></td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td><strong>Endorsing Body:</strong></td>
<td>Healthcare Quality Assurance and Improvement Committee</td>
</tr>
<tr>
<td><strong>Governance or Assurance Committee:</strong></td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td><strong>Implementation Date:</strong></td>
<td>September 2010</td>
</tr>
<tr>
<td><strong>Version Number:</strong></td>
<td>2.6.5</td>
</tr>
<tr>
<td><strong>Review Date:</strong></td>
<td>September 2020</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Contributing Author / Authors</th>
<th>Alan Ashforth, Information Security Manager, eHealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultation Process / Stakeholders:</td>
<td>Donald Wilson, Director of Information and Digital Technology &amp; Senior Information Risk Owner (SIRO)</td>
</tr>
<tr>
<td></td>
<td>Information Governance Committee members</td>
</tr>
<tr>
<td>Distribution:</td>
<td>All staff</td>
</tr>
</tbody>
</table>

## CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2006</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Mar 2007</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Sept 2010</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>2.0</td>
</tr>
<tr>
<td>July 2013</td>
<td>A Ashforth</td>
<td>Revised in view of comments</td>
<td>2.2</td>
</tr>
<tr>
<td>May 2014</td>
<td>A Ashforth &amp; C Tannahill</td>
<td>Revised in view of comments</td>
<td>2.3</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>A Ashforth &amp; C Tannahill</td>
<td>Main change - Insertion of new sub-section – Single Sign On</td>
<td>2.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor change - Reference appendix updated</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor change - some rewording throughout</td>
<td></td>
</tr>
<tr>
<td>Aug 2015</td>
<td>A Ashforth</td>
<td>Minor change - Reference appendix</td>
<td>2.5</td>
</tr>
<tr>
<td>Aug 2016</td>
<td>A Ashforth</td>
<td>Minor change – Update to describe password complexity in General section and Appendix 2</td>
<td>2.5.1</td>
</tr>
<tr>
<td>Nov 2016</td>
<td>A Ashforth</td>
<td>Minor change – Include references to and section on “Third party suppliers” within policy principles wording.</td>
<td>2.5.3</td>
</tr>
<tr>
<td>April 2017</td>
<td>A Ashforth</td>
<td>Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.</td>
<td>2.5.4</td>
</tr>
<tr>
<td>April 2018</td>
<td>A Ashforth</td>
<td>Reviewed in line with General Data Protection Regulation (GDPR)</td>
<td>2.6</td>
</tr>
<tr>
<td>May 2018</td>
<td>A Ashforth</td>
<td>Change to Principle Content – General section – ‘Passwords must consist of a minimum of 8 characters’</td>
<td>2.6.1</td>
</tr>
</tbody>
</table>
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 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 Third Party Suppliers who support NHS Lanarkshire eHealth 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.

Passwords must consist of a minimum of 8 characters and needs to conform with complex password rules. Password complexity requires a password that contains at least one uppercase character, one lowercase character and one number. It is recognised that hackers using 'password crackers' are capable of very many password probes in a short period of time. The most effective passwords are therefore those with the longest number of characters.

Staff should not disclose their passwords to any other person, even eHealth 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. “efin”.

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
Information Security Policy – Secure Use of Passwords

either the system being accessed or the background of the user and can be guessed by potential intruders.

Password Maintenance
Re-use of recent passwords is not allowed.

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

Single Sign On
Staff may already 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.

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

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 eHealth 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 eHealth assets managed by Third Party Suppliers is subject to NHS Lanarkshire’s eHealth Change Control 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

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:

- General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- 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
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
12. Appendix 2 – Summary of Good Password Practice

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
- Network passwords must conform with password complexity. Your network password must contain at least one uppercase character, one lowercase character and one number.
- **Do not** choose a password that relates directly to the system intended to be accessed
- Seek advice from the IT 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 IT Service Desk for assistance
- If you suspect your password has been used by others contact the IT Service Desk so that the incident can be investigated