### Summary:
This document describes the information security requirement for the use of passwords to access Southern Health NHS Foundation Trusts (the Trust) information systems.

### Keywords (minimum of 5):
(To assist policy search engine)
- Passwords
- Protection
- Passphrase
- Account
- Credentials

### Target Audience:
All staff employed by Southern Health NHS Foundation Trust. Non-Executive Directors, Volunteers, Governors and Contractors

### Next Review Date:
September 2021, or earlier if required.

### Approved and Ratified by:
Information Governance Group  Date: 09/09/2019

### Date issued:
September 2019

### Author:
Edward Purcell – IT Security Specialist

### Accountable Executive Lead:
Finance Director
## Version Control

### Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Page</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>25/07/2012</td>
<td>Adam Newman</td>
<td>1.0</td>
<td>All</td>
<td>First issue</td>
</tr>
<tr>
<td>11/02/2016</td>
<td>Edward Purcell</td>
<td>2.0</td>
<td>All</td>
<td>Review and updated by EP. Changes made in response to feedback from P. Ballard and A. Young.</td>
</tr>
<tr>
<td>12/07/2018</td>
<td>Edward Purcell</td>
<td>3.0</td>
<td>All</td>
<td>Increase of password length from 8 characters to 10 in response to a recent security audit. All content reviewed for accuracy including updates to reflect GDPR.</td>
</tr>
<tr>
<td>05/09/2019</td>
<td>Edward Purcell</td>
<td>3</td>
<td>All</td>
<td>Reviewed policy, no changes. Updated front cover</td>
</tr>
</tbody>
</table>

### Reviewers/Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Version Reviewed &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Group</td>
<td>Membership –sign off</td>
<td>1.0 – 03/12/2012</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership –sign off</td>
<td>2.0 – 04/03/2016</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership –virtual sign off</td>
<td>3.0 – 12/07/2018</td>
</tr>
<tr>
<td>Information Governance Group</td>
<td>Membership –sign off</td>
<td>3 – 09/09/2019</td>
</tr>
</tbody>
</table>
## Contents

1. Introduction ......................................................................................... 4  
2. Scope .................................................................................................. 4  
3. Duties / Responsibilities .................................................................... 4  
4. Password Policy .................................................................................. 5  
5. Password Protection Standards .......................................................... 6  
6. Passphrases ....................................................................................... 7  
7. New User Credentials ......................................................................... 8  
8. Password Reset Process ..................................................................... 8  
9. Training Requirements ....................................................................... 8  
10. Policy Review .................................................................................... 8  
11. Associated Documents ...................................................................... 8
IT Password Protection Policy

1. Introduction

1.1. Security best practice demands that access to IT resources is properly controlled and auditable. The front line of protection for user and system accounts is the use of a password. Poorly chosen passwords, or the failure to enforce a requirement for complex passwords, may result in the compromise of an entire network and associated services.

1.2. The risk to the Trust is quantified as both financial and reputational and the failure to implement a robust password policy could result in a security breach with the subsequent loss of information. Any breach is reportable to the Information Commissioners Office (ICO) who has the ability to impose penalties of up to 10 million euros or 2 per cent of global turnover for the most serious failing. In addition, details of ICO investigations are made public which would lead to reputational damage.

1.3. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the frequency of change, enforcement of policy and to provide guidance on the application of password policy on all equipment, applications and levels of user throughout the Trust.

2. Scope

2.1. This policy applies to all staff authorised to use Trust computer systems and communications networks whether they are employed directly by the Trust, contractors, NHS Professionals, bank staff, voluntary organisations or suppliers granted access for support purposes.

3. Duties / Responsibilities

3.1. The Information Technology Department and any contracted third parties have the responsibility of ensuring that all passwords are in line with this policy.

3.2. The IT Department is responsible for:
   - ensuring that all hosted domain/application/system passwords are in line with this policy.

3.3. All Information Asset Owners (IAO) are responsible for:
   - ensuring the principles outlined within this password protection policy are applied to the information assets for which they are responsible, including those which are externally supported and/or hosted.

3.4. All Trust staff, without exception, must:
   - abide by this and associated policies & procedures;
   - report the breach, misuse or sharing of passwords to the IT Service Desk.
   - change their assigned password after successfully logging on for the first time or if a compromise is suspected;
never disclose their individual account password to anyone, including other Trust computer account holders.

use complex password as described in this policy and not repeat or re-use a password within a 12 month period;

change their passwords regularly and not attempt to exceed the enforced 90 day period.

4. **Password Policy**

4.1. All passwords or password files stored on equipment or within applications are to be stored with one way encryption.

4.2. Password characters are not to be displayed on screen when typed into logon screens.

4.3. User passwords should not be disclosed via electronic means e.g. inserted into email messages, unless encrypted channels are used.

4.4. After account generation, or when a user has requested a password reset, the account must be set to force the user to select their own password when first accessing the system after this event.

4.5. If an account or password compromise is suspected, report the incident to the IT Security Team via the IT Service Desk and complete an incident on Ulysses as per the incident reporting policy.

4.6. All users that require privileged access should have an alternate and unique account with a separate password from their normal user account.

4.7. All Active Directory (AD) passwords (and others where appropriate) shall lock after 5 consecutive invalid attempts to use them.

4.8. The password lock shall remain in-place for 10 minutes. (This means the lock placed after five invalid attempts will be removed after 10 minutes; resetting a password will automatically remove this lock).

4.9. Only complex passwords are to be utilised and these should follow the guidelines outlined and should relate to the type of account (user-level, system-level and service account) as defined in the policy below.

4.10. **User-Level Passwords**

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days. If a password becomes compromised it should be changed immediately.

- All user level passwords will meet (or exceed) a minimum length of 10 characters;

- All user level password shall be complex and contain at least three of the four following character classes:
  - Uppercase characters (A - Z)
  - Lower case characters (a – z)
  - Numbers (0 through 9)
6

SH IG 30 IT Password Protection Policy
Version: 3
September 2019

- Special characters (@#$%^&*()_+\|~-=\[];":'<> / etc.)

- All systems must retain a password history of the last 4 passwords used.

- All user level passwords are required to be kept for at least one day, to prevent users immediately cycling through passwords and returning back to their original password.

4.11. **System-Level Passwords**

- All system-level passwords (e.g., root, Windows Administrator, application administration accounts, etc.) provide complete control over a system and must be changed on at least every 180 days.

- All system-level passwords a minimum length of 10 characters.

- All system-level passwords shall be complex and contain at least three of the four following character classes:
  - Uppercase characters (A - Z)
  - Lower case characters (a – z)
  - Numbers (0 through 9)
  - Special characters (@#$%^&*()_+\|~-=\[];":'<> / etc.)

- System-level passwords generally have higher privileges associated to them and should only be used when the additional rights that the account provides is needed.

- All production system-level passwords must be part of the security administered password store.

- System-level passwords must not be disclosed outside of the department.

4.12. **Service Account Passwords**

- Non-expiring passwords are permitted for service accounts only.

- Service accounts passwords should be changed at least every 6 months, unless it becomes compromised before the review date when it should be changed immediately.

- All production service account passwords must be part of the security administered password store.

5. **Password Protection Standards**

5.1. **Poor, weak passwords** have the following characteristics:

- The password contains less than 10 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
5.2. **Strong passwords** have the following characteristics:

- Contain both upper and lower case characters (e.g., A-Z, a-z).
- Have digits and punctuation characters as well as letters e.g., 0-9!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- Are at least eight alphanumeric characters long and a passphrase (e.g., Ohmy1stubbedmytoe).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should not normally be written down or stored on-line. Individuals should try to create passwords that can be easily remembered.

5.3. Do not use the same password for work accounts as for non-work related accounts (e.g., personal ISP account, social networking account, on-line banking, etc.).

5.4. Where possible, don't use the same password for various work access needs. For example, select one password for the clinical systems and a separate password for network accounts. Also, select a separate password to be used for an NT account and a UNIX account.

5.5. Always consider declining the use of the "Remember Password" feature of applications.

5.6. In no circumstance should any user share his or her password with any other person, including management, IT department, Information Governance, third-party or trusted friends. Likewise no person employed or contracted within the Trust should ask another person for his or her password or logon credentials.

5.7. If someone demands a password, refer them to the relevant policy and raise the call to the IT security team via the IT Service Desk.

6. **Passphrases**

6.1. Passphrases are generally used for public/private key authentication but may be used instead of a password for all user accounts. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

6.2. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

6.3. A good passphrase is relatively long and includes several random words or abbreviations to make it easier to remember eg 'Headbeerleg!', 'teethPhon3pen'. The passphrase must contains a combination of upper and lowercase letters and numeric and punctuation characters.

6.4. All of the rules above that apply to passwords apply to passphrases.
6.5. Passphrases should be used in preference to Passwords wherever possible, particularly for generating certificates, shared secrets and wireless keys (if required, see wireless policy).

7. **New User Credentials**

7.1. In the case of new AD user accounts and when the new user’s line manager is clearly identified then the user credentials will be emailed internally to the line manager of the new user i.e. the individual authorising the creation of the new user account.

7.2. Where a new user is also granted access to applications that have user credentials these details may be emailed internally to the new users email account.

8. **Password Reset Process**

8.1. Where the service desk is able to verify a user then a password resets can be administered over the phone following the service desk procedure.

8.2. In cases where the service desk is not involved then password resets are normally to be granted on a face to face or written basis as per notification of new user credentials.

8.3. A self-service password reset tool is currently available to staff who have a requirement – for example, their working hours are outside helpdesk hours – and this facilitates AD password reset through answering a series of pre-registered secret questions.

8.4. **Enforcement**

8.5. Any employee found to have violated this policy may be subject to disciplinary action.

9. **Training Requirements**

9.1. Information Governance Annual Training is required annually for all staff and this includes a section on Information security which covers password protection.

9.2. IT Support staff must be conversant with the appropriate standards and guidelines referenced by this policy.

10. **Policy Review**

10.1. This policy shall be reviewed every 3 years, or more frequently if required.

11. **Associated Documents**

- IT Security Policy
- IT Account Policy and Standards