NHS
Leeds
Clinical Commissioning Group

Password Management Policy

Version:	1
Ratified by:	Audit Committee
Date ratified:	March 2022
Name & Title of originator/author:	Abi Dakin, Cyber Assurance and Compliance Lead
Name of responsible committee/individual:	Information Governance Committee
Date issued:	Sept 2020
Review date:	March 2024
Target audience:	All staff, Volunteers, Contractors

Executive Summary

The Password Management Policy encompasses an assortment of methods in which to competently manage a robust and effective security system with regards to protecting personal data and computer systems.

It outlines the need for well thought out password protection and the risks associated with failing to do so. The policy has been developed and reviewed in line with developments within the Information Governance agenda.

Equality Impact Assessment (EIA)

This document has been assessed, using the EIA toolkit, to ensure consideration has been given to the actual or potential impacts on staff, certain communities or population groups, appropriate action has been taken to mitigate or eliminate the negative impacts and maximise the positive impacts and that the and that the implementation plans are appropriate and proportionate.

Contents

1 Introduction

This protocol is part of a set of Information Management and Governance policies and procedures that support the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies, in particular the Information Assurance Policy and the Acceptable Use Protocol. A failure to comply with this protocol could lead to an inability to collect and present legally admissible evidence and a breach of our legislative, regulatory and/or contractual requirements, including the General Data Protection Regulations, Data Protection Act 2018 and the Data Security and Protection Toolkit.

2 Scope

This protocol applies to the CCG Network ID specifically. To everyone who has access to CCG information, electronic information assets, systems, applications or IT equipment. These people are referred to as 'users' in this protocol. This may include, but is not limited to all employees, consultants, contractors and agents employed by Leeds CCG who are provided with authorised access to the CCG equipment, systems or information. All those who use or have access to CCG information must understand and adopt this protocol and are responsible for ensuring the security of the CCG's information systems and the information that they use or handle.

This protocol relates to the authentication to all Information Systems (IS) environments operated by Leeds CCG or contracted with a third party for use by Leeds CCG, however it is specifically for the CCG Network ID.

3 Purpose

The objective of this protocol is to ensure that Leeds CCG has adequate controls for access to systems and data via user-challenge or 'password', and that users understand their responsibilities with regards to password use. This protocol establishes a standard for creating and maintaining passwords. Standards and guidance produced by the National Cyber Security Centre (NCSC) suggests that using a longer password that never need be changed discourages a person to reuse passwords and encourages them to commit it to memory.

4 Password disclosure

Users SHALL NOT, under any circumstances, share or disclose their password. Password disclosure is deemed a serious security matter and will be dealt with under the CCG's Disciplinary procedure, which may include dismissal.

5 General rules for Passwords

Your CCG password SHALL only be used for your CCG network ID.
Users MUST NOT write their passwords down under any circumstances.
Well known phrases or lyrics shall NOT be used.
If you believe your password has been compromised by another user, use control/alt/delete to change your password as soon as you are able and report it to the Service Desk.

6 Password Length

- All user level passwords must be at least twelve (12) characters long.
- Systems/ADM raised privilege accounts passwords should be at least sixteen (16) characters long.
- Ideal passwords are a series of multiple random words that will be remembered by the user, separated by a symbol (e.g. “Retro-kettle-ship”). This helps balance security with memorability.

7 Password Complexity

Active Directory passwords must include at least 2 of 3 complexity characters (Capital letter, Numbers or Special character)

8 Brute Force Protection

To mitigate against brute-force attacks, passwords shall NOT:

Brute force attacks are used by hackers to quickly guess passwords by using a database of known, common passwords.

- Include any element of the user’s name, payroll number or log-in ID, nor the name of any team, or other identifier that relates to the user or of Leeds CCG.
- Be left as a default or generic system password.
- Include known, easily guessable phrases: “Letmein****”, “password***”, etc.
- Include common names such as family members, pets, friends, co-workers, celebrities, famous historical figures, etc.
- Include system or application terms and names, commands, sites, companies, hardware or software (e.g. “MicrosoftWindows10”, “CCGPassword2”).
- Include personal information, addresses, birthdays, email, phone numbers, etc.
- Patterns such as abcdef, ASDFGH, zyxwvuts, 123321, 123456, 98765…etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

An Audit of passwords shall be carried out in order to address passwords not meeting this protocol.

Technical controls shall lockout any user who makes ten (10) failed attempts to enter their password.

9 Password Expiry

Passwords will expire and need to be changed after 365 days

10 Password History

Users shall NOT reuse previous passwords as this carries a risk that previous passwords were breached.

Technical controls will prevent the reuse of passwords to 10 instances.

11 Creation of Passwords

Password generation tools are available on the internet and should be used to provide a random, memorable series of words to be separated by spaces or characters. This follows guidance produced by the National Cyber Security Centre (NCSC) and is considered best practice.

12 Non Compliance

If you fail to comply with this protocol you may be referred and subject to the Disciplinary Policy and Procedure. A potential outcome of disciplinary action could result in your dismissal with or without notice or payment in lieu of notice

13 Auditing

System access logons are recorded in event logs, whether these are successful or not. These logs are maintained for a period of time and unsuccessful attempts are noted and monitored. These logs can be used to ascertain breaches in security and to determine the person responsible.

14 Monitoring Compliance and Effectiveness

Staff are expected to comply with the requirements set out within the Password Protocol and related policies. Compliance will be monitored via, completion of staff questionnaires, incidents reported, electronic audit trails.

Non adherence to the Password Management Policy and related policies will result in local Disciplinary Policies being implemented.

Policy Consultation Process:

Title of document	Password Management Policy
Author	Abi Dakin, Cyber Assurance and Compliance Lead
New / Revised document	New
Lists of persons involved in developing the policy List of persons involved in the consultation process:	Abi Dakin Carrick Armer Karen Rowe IG Committee