North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

IT Services - Password Policy

As the South, Central & West Commissioning Support Unit (SCW) provides IT networks, equipment and support to North Hampshire CCG, all CCG employees are required to adhere to the CSU IT Services information security policies. The following policy was developed by the CSU IT Services Team and adopted for use by the CCG.

This document can be made available in a range of languages and formats on request to the policy author.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Andy Ferrari – Head of IT Strategy and Planning
Name of responsible committee/individual:	IT Services Leadership Team
Name of executive lead:	Suzanne Tewkesbury – Director of Corporate Development & Performance
Date issued:	09/01/2018
Review date:	25/05/2018
Target audience:	South, Central & West CSU staff and Customers

Document Control Sheet

Title	**IT Services - Password Policy**
Version	2.1
Status	Approved – Final
Author	Andy Ferrari
Date Created	19/01/2016
Date Last Updated	14/12/2017

History			
Version	**Date**	**Author(s)**	**Comments**
0.1	19/01/2016	Andy Ferrari	Initial SCW draft based on Stuart Collier's South CSU heritage document
1.0	02/02/2016	Andy Ferrari	Updated following comments from SCW Information Governance Group and approval from SCW Corporate Governance Assurance Group
1.1	08/09/2016	Arif Gulzar	Updated policy review date and some minor changes
1.1	04/10/2016	Arif Gulzar	Policy signed off by Information Governance Steering Group
2.0	29/11/2016	Arif Gulzar	Version reset after ratification from Corporate Governance Assurance Group
2.1	14/12/2017	Arif Gulzar	Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	Title and contact
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1 Introduction

This document forms part of the NHS South, Central and West Commissioning Support Unit (SCW) Information Security Management System.

This document provides detailed policies that govern the usage of passwords.

1.1 The Information Security Management System (ISMS)

The objective of the ISMS is to define a coherent set of policies, standards and architectures that:-

- Set out the governance of IT security.
- Provide high level policy statements on the requirements for managing IT security.
- Define the roles and responsibilities for implementing the IT security policy.
- Identify key standards, processes and procedures to support the policy.
- Define security architectures that encapsulate the policy and support the delivery of secure IT services.

1.2 Document Purpose

This document provides the detailed password policy statements that support the overall IT security objectives of the CSU as set out in the security statement in the ISMS.

2 Password Policy [i] [ii] [iii]

2.1 Policy Overview

The policy describes how users of SCW supported systems should create and manage their passwords. This policy applies to all systems, including those which currently do not have an enforced password change process.

2.2 Policy Audience

This policy applies to all SCW employees including temporary staff, sub-contractors, contractors and third parties with access to SCW information, information systems and services. In this document the audience described here will be referred to as users.

2.3 Policy Detail

- Users must not write down their password.
- Users must not disclose their password by any means.
- Users must choose a password that is not easily guessed by others, for example the following are **not** suitable – dictionary words, car makes, telephone & room numbers; forenames and surnames; common words e.g. colours, seasons, days, sports, beverages etc.; simple keyboard sequences e.g. qwerty; words associated with computers.
- SCW logon passwords must be changed every two months (automatically enforced). Where enforced changes are not present, the user should manually change the application password.
- Passwords must have a minimum of 8 characters.

  It is acknowledged that most tablets and smartphones issued by SCW are currently protected by four-character passwords pending a solution for these devices to comply with this policy.
- Users must ensure their SCW password is different from any other passwords they use to access non-SCW systems or devices.
- Users must ensure that password consists of a mix of at least 3 of the following types of characters:

  alpha (uppercase),

  alpha (lowercase),

  numeric characters and

special characters (i.e. punctuation).

- System level passwords (e.g. Root, Administrator, Service Accounts) must be stored within an encrypted password vault.
- Privileged users should be provided with an alternative account with a password different to their standard login.
- Should a password be compromised it should be changed immediately and the SCW IT Service Desk informed.
- Under no circumstances should the logon or password be shared. The sharing of passwords is considered a serious disciplinary offence and will be dealt with accordingly.
- All users are responsible for reporting any suspected misuse of passwords.

2.4 Policy Non-Compliance

Any breach of this policy could result in disciplinary action and possible ICO action if information loss occurs.

3 Review of Policy

3.1 Review Timetable

As part of the Information Security Management System this policy will be reviewed on an ongoing basis by the CSU ICT senior management team.

[i] A 11.2.3 User password management
[ii] A 11.3.1 Password use
[iii] A 11.5.3 Password management system