OFFICIAL

Password Policy
Version 3

South, Central and West Commissioning Support Unit
July 2018

DOCUMENT CONTROL

Document Name	Version	Status	Author
Password Policy	*3.0*	*Final*	*Associate Director of Strategy and Planning*

Document objectives:	*This policy is designed to protect the resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.*	
Target audience:	*All staff*	
Committee/Group Consulted*:*	*SCW Information Governance Steering Group*	
Monitoring arrangements and indicators:	*This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.*	
Training/resource implications:	*All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet corporate IT policies pages*	
Approved and ratified by:	*SCW Information Governance Steering Group* *SCW Corporate Governance Assurance Group*	*Date: 24 July 2018*
Equality Impact Assessment:	*Yes*	*Date: 23 July 2018*
Date issued:	*24 July 2018*	
Review date:	***July 2019***	
Author:	*Associate Director of Strategy and Planning*	
Lead Director:	*Director of IT Services*	

Version Control

Date	Author	Version	Page	Reason for Change
19/01/2016	Andy Ferrari	0.1		Initial SCW draft based on Stuart Collier's South CSU heritage document
02/02/2016	Andy Ferrari	1.0		Updated following comments from SCW Information Governance Group and approval from SCW Corporate Governance Assurance Group
08/09/2016	Arif Gulzar	1.1		Updated policy review date and some minor changes

04/10/2016	Arif Gulzar	1.1		Policy signed off by Information Governance Steering Group
29/11/2016	Arif Gulzar	2.0		Version reset after ratification from Corporate Governance Assurance Group
14/12/2017	Arif Gulzar	2.1		Extended policy review date to align with GDPR after approval from SCW Information Governance Steering Group
18/05/2018	Arif Gulzar	2.2	All	Updated policy template with corporate branding.
21/05/2018	Arif Gulzar	2.3		Policy reviewed and approved by IT senior leadership team.
24/07/2018	Arif Gulzar	3.0		Version changed after CGAG ratification

Reviewers/contributors

Name	Position	Version Reviewed & Date
Simon Sturgeon	Director of IT Services	V2.2 21/05/18
Andy Ferrari	Associate Director of IT Strategy and Planning	V2.2 21/05/18
Cathy Jukes	Associate Director of IT Projects and Programmes	V2.2 21/05/18
Michael Knight	Associate Director of Technology Management and Architecture	V2.2 21/05/18
David Walch	Head of IT Service Delivery	V2.2 21/05/18
Stephanie Wilson	Head of Service Development and Support	V2.2 21/05/18

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 SCW as set out in the security statement in the ISMS.

2 DETAILS OF THE PASSWORD POLICY

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, third parties and customers 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 passwords is considered a serious disciplinary offence and will be dealt with accordingly.
- All users are responsible for reporting any suspected misuse of passwords.

3 *PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT*

The Equality Act 2010 requires public bodies to consider the needs of all individuals in their day to day work. At SCW we do this by completing an Equality Impact Assessment as described in the Equality and Diversity Policy which can be found, along with the assessment form, on the ConsultHR intranet site. If you need help identifying potential equality issues you should contact SCW's equality and diversity lead.

4 POLICY NON-COMPLIANCE

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

5 REVIEW OF POLICY

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

APPENDIX A - EQUALITY IMPACT ASSESSMENT

For IT Password Policy

1. Title of policy/ programme/ framework being analysed

IT Password Policy.

2. Please state the aims and objectives of this work and the intended equality outcomes. How is this proposal linked to the organisation's business plan and strategic equality objectives?

To provide a framework of guidance to NHS South, Central and West CSU (SCW) staff (as defined in the scope) regarding the security of Personal and Sensitive Data in both paper and electronic form.

3. Who is likely to be affected? e.g. staff (as defined in the scope), patients, service users, carers

Staff.

4. What evidence do you have of the potential impact (positive and negative)?

None expected.

4.1 Disability (Consider attitudinal, physical and social barriers)

No impact

4.2 Sex (Impact on men and women, potential link to carers below)

No impact

4.3 Race (Consider different ethnic groups, nationalities, Roma Gypsies, Irish Travellers, language barriers, cultural differences).

No impact

4.4 Age (Consider across age ranges, on old and younger people. This can include safeguarding, consent and child welfare).

No impact

4.5 Gender reassignment (Consider impact on transgender and transsexual people. This can include issues such as privacy of data and harassment)

No impact

4.6 Sexual orientation (This will include lesbian, gay and bi-sexual people as well as heterosexual people).

No impact

4.7 Religion or belief (Consider impact on people with different religions, beliefs or no belief)

No impact

4.8 Marriage and Civil Partnership

No impact

4.9 Pregnancy and maternity (This can include impact on working arrangements, part-time working, infant caring responsibilities).

No impact

4.10 Carers (This can include impact on part-time working, shift-patterns, general caring responsibilities, access to health services, 'by association' protection under equality legislation).

No impact

4.11 Additional significant evidence (See Guidance Note)

Give details of any evidence on other groups experiencing disadvantage and barriers to access due to:

- socio-economic status

• location (e.g. living in areas of multiple deprivation) • resident status (migrants) • multiple discrimination • homelessness No impact
5. Action planning for improvement (See Guidance Note) Please give an outline of the key action points based on any gaps, challenges and opportunities you have identified. An Action Plan template is appended for specific action planning.
Sign off
Name and signature of person who carried out this analysis Beverly Carter Head of IG, NHS South, Central and West Commissioning Support Unit
Date analysis completed 23 July 2018
Name and signature of responsible Director Simon Sturgeon, Director of IT Services
Date analysis was approved by responsible Director 23 July 2018

Document Ends