OFFICIAL

Access Control Policy
Version 3

South, Central and West Commissioning Support Unit
July 2018

DOCUMENT CONTROL

Document Name	Version	Status	Author
Access Control Policy	*3.0*	*Final*	*Cyber Security Manager*
Document objectives:	*The objective of this policy is to prevent unauthorised access to SCW, and its customer's information systems and network. The policy will describe how access controls are applied by the organisation, covering all stages in the life-cycle of user access, from the initial registration process of new users to the final de-registration of users who no longer require access to information systems and services.*		
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:	*Cyber Security Manager*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
06.01.2014	Stuart Collier	0.1		Draft

08.01.2016	Phill Wade	1.0		SCW CSU Updates and version reset
06.09.2016	Arif Gulzar	1.1a		Updated policy review date and sections 4.5,5.2,5.4,5.5,6 & 9
04.10.2016	Arif Gulzar	1.1b		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
14/05/2018	Arif Gulzar	2.2	All	Updated corporate policy template with corporate branding. Updated section 3.1. with DSP Updated section 3.2. with GDPR and added legislations Updated section 4 with roles and responsibilities aligned with other policies and GDPR
21/05/2018	Arif Gulzar	2.3		Policy reviewed and signed off 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 5
1.1 The Information Security Management System (ISMS) 5
1.2 Document Purpose 5
2 Objectives 5
3 Scope of the Access Control Policy 6
3.1 Definition 6
3.2 Legal Requirements 7
4 Roles and Responsibilities 8
5 User Access Management 10
5.1 New User 10
5.2 De-Registration of Users – Revoking Access Rights 11
5.3 New Remote Users 11
5.4 Privilege Management 11
5.5 User Password Management 12
5.6 Review of User Access Rights 12
5.7 Change of User Requirements 12
6 Monitoring and Audit 13
7 Policy Review 13
8 Dissemination and Implementation 13
9 Related Documents Policies and Procedures 14
APPENDIX A - Equality Impact Assessment 15

1 Introduction

This document defines the Access Control Policy for NHS South, Central and West Commissioning Support Unit (SCW). The Policy applies to all staff (including temporary, contract, third party and agency staff) working for, on behalf of, or whose organisation that has entered into an agreement for the provision of IT services by the SCW.

Access Control policy is a key component of the SCW overall information security management framework and this policy should be read in conjunction with other SCW's information security documentations including security guidance, protocols, policies and procedures.

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 IT Access Control policy statements that support the overall IT security objectives of the SCW as set out in the security statement in the ISMS

2 Objectives

The objective of this policy is to prevent unauthorised access to the SCW, and its customer's information systems and network. The policy will describe how access controls are applied by the organisation, covering all stages in the life-cycle of user access, from the initial registration process of new users to the final de-registration of users who no longer require access to information systems and services.

3 Scope of the Access Control Policy

This Policy covers all devices owned by or connected to the SCW IT Network at any site owned or leased by the organisation or from a remote location from where users connect to this network. The scope of this policy covers the following:

- Provision of authorisation and access to network services
- Secure authentication (smartcards, passwords)
- Remote access (3G, VPN)
- Suppliers and other third party access
- Wireless access (Wi-Fi)
- Access for patients

3.1 Definition

CD-ROM	Compact Disc Read-only Memory
IT	Information & Communication Technology
DCs	Data Custodians
IAO	Information Asset Owner
DSP	Data Security and Protection Toolkit
ISO	International Standard Organisation
VPN	Virtual Private Network
IT	Information & Technology
ITSEC	Information Technology Security Evaluation Criteria
SIRI	Serious Incidents Requiring Investigation
SIRO	Senior Information Risk Officer

3.2 Legal Requirements

The legal framework on which this access control policy and other related information security policies are based is as follows;

All SCW staff are required to ensure compliance with Data Protection Legislation. This includes:

- the General Data Protection Regulation (GDPR)
- the Data Protection Act (DPA) 2018
- the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including:

- the Human Rights Act 1998
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations

Consideration must also be given to the:

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008

- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Digital Economy Act 2010 and 2017
- Counter-Terrorism and Security Act 2015

4 Roles and Responsibilities

SCW Managing Director

SCW Managing Director has overall responsibility for Information Governance within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

SCW Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for SCW is an executive management team member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at executive management level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SCW Information Governance Team will support the SIRO in fulfilling this role.

SCW Caldicott Guardian

The Caldicott Guardian is the person within SCW with overall responsibility for protecting the confidentiality of information that includes personal data and special categories of personal data, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the SCW Executive Management Team on confidentiality issues. SCW Information Governance Team will support the Caldicott Guardian in fulfilling this role.

SCW Deputy Data Protection Officer

The Deputy Data Protection Officer (DDPO) is the person within SCW that has been identified to support the role of the Data Protection Officer (DPO) in NHS England. This role has the responsibilities as set out in the GDPR guidance as delegated duties

from the DPO and is responsible to feedback any Information Governance issues to SCW Executive Management Team and the DPO at NHS England. The DDPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident. They will also be part of the Data Protection Impact Assessment (DPIA) process on behalf of SCW.

SCW Information Governance Team

SCW Information Governance Team is responsible for ensuring that the Information Governance programme is implemented throughout the organisation. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit for SCW. The Information Governance Team will support the organisation in investigating Serious Incidents Requiring Investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols.

SCW Information Asset Owners (IAO)

The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what data and information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The Information Governance Team will support the IAOs in fulfilling their role.

SCW Data Custodians (DC's)

Data Custodians are required to support the IAO's and SCW SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. The Information Governance Team will provide local face to face IG training if required and will monitor staff compliance by way of the consult OD portal and link to the e-LfH platform.

Cyber Security Manager

Responsibilities of the Cyber Security Manager include:

- Acting as a central point of contact on IT security within the organisation and for external organisations that has entered into an agreement for the provision of IT services by SCW.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.

- Advise on the content and implementation of the Information Security Programme.
    - Co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures.
    - Liaise with external organisations on IT security matters, including representing the organisation on cross-community committees.
    - Advising users of information systems, applications and Networks of their responsibilities.
    - Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
    - Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
    - Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

All Staff

All staff working for, on behalf of, or whose organisation that has entered into an agreement for the provision of IT services by SCW have a general responsibility for the security of information they create or use in the course of their duties. They should ensure they are aware of all the relevant information security policies and procedures and follow their recognised codes of conduct. NHS staff have a legal duty of confidentiality to keep information about individuals confidential.

5 User Access Management

5.1 New User

The life-cycle of user access, from the initial registration process of new users to the final de-registration of users who no longer require access to information systems and services is controlled through a formal user registration process beginning with a formal completion of the New User Form, which can be found on SCW IT service desk portal webpage or on request from the local IT Service Desk.

All requests for access must be made by using the online or word template application forms with a section completed by the user's line manager.

There is a standard level of access (Network, Email and Internet), other services can be accessed when specifically authorised by the responsible SCW IT.

5.2 De-Registration of Users – Revoking Access Rights

Within 5 days of the IAO or line manager advising the IT team that a user has left the organisation/employment, all associated system logins will be revoked.

In accordance with the employee/contract termination process it is the responsibility of the line manager to complete the Leaver Form and ensure that the user is de-registered from the SCW systems and services. The request should be made in advance of the user's last day and specify a date and time for access to be revoked upon the user leaving.

Providing the requesting manager can be positively identified, the requests must be actioned within 5 days by IT Services.

IT Services should keep a record of all de-registration requests and file the original forms with all previous requests for that user.

5.3 New Remote Users

The privilege of remotely accessing the SCW systems and services from non-NHS sites, including private homes, may be granted to fulfil business needs. Application should be made using the Remote Access Request form.

The requirements for remote user registration and de-registration remain the same as standard network users.

5.4 Privilege Management

"Special privileges" are those allowed to the System Administrators and their deputies allowing global access to their systems for the purpose of performing their administrative duties. This access may or may not include access to some or all data. The unnecessary allocation and use of special privileges is a major contributing factor to system vulnerability.

Therefore, special privileged access is to be strictly controlled and recorded for all major electronic Information Assets and only permitted to ensure business continuity. System Administrators and their deputies may only grant a user special privileged

access when specifically authorised by the Caldicott Guardian responsible for the asset.

5.5 User Password Management

Password format and general rules are set out in SCW's information security documentations including the IG Staff Handbook & IT Password Policy.

Where a user has forgotten their password, the System Administrator or the IT Service Desk is authorised to issue a replacement, which must be changed by the user on logon.

Upon receipt of such a request the System Administrator/Service Desk will:

1. Ensure the request is logged.
2. Confirm the identity of the user by physical recognition or on successful completion of a series of predefined question and answers unique to each user.

5.6 Review of User Access Rights

Each System Administrator or deputy will conduct a review of all access rights to the network they are responsible for, at least once a quarter in conjunction with the IAOs. This action will positively confirm all current users. Any user accounts, which cannot be positively identified as current, must be disabled immediately, pending deletion. However, to allow for maternity leave or other extended absence, the System Administrator should check the status of users with their IAOs or line managers before deleting inactive accounts after one month.

5.7 Change of User Requirements

Change of user requirement requests will normally relate to additional services or an alteration to the access level for particular applications. This is often the result of internal movement of staff or changes to existing roles. As per new user registration, IAOs or line managers should initiate and authorise the request which should be clearly annotated 'Change for Existing user', to avoid creating multiple accounts for single users.

System Administrators will make the requested changes only after receipt of a properly completed request form, providing the appropriate procedures have been complied with and the access criteria met.

System Administrators will keep a record of all change requests and file the original forms with all previous requests for that user.

6 Monitoring and Audit

In order to provide assurances that controls in place are working effectively, the Cyber Security Manager will work closely with SCW IG and external auditors to ensure that audits of systems and networks are conducted on a regular basis.

Any breaches in will be identified and reported, initially logged as a call via the IT Service Desk and where appropriate an Incident being raised and investigated as per each organisation's guidelines.

7 Policy Review

In line with the SCW's key documents, this policy will be reviewed no later than 2 years from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review.

Awareness of any new content or change in process will be through electronic channels e.g. through email, in staff bulletins etc. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SCW IG and IT Services teams.

8 Dissemination and Implementation

This policy will be published on the SCW intranet. IAOs and line managers are required to ensure that their staff understands its application to their practice.

Organisations that have entered into an agreement for the provision of IT services by the SCW should ensure that this document and other IT related documents are cascaded to their staff.

9 Related Documents Policies and Procedures

The following documentation relates to the management of information and together underpins the SCW's Information Governance Assurance Framework. This procedure should be read in conjunction other policies:

- Information Governance Framework Policy
- Information Security Policy
- IT Services - Security Incident Handling Policy and IG Incident Management Policy
- Network Security Policy
- Business Continuity Plans

APPENDIX A - EQUALITY IMPACT ASSESSMENT

For IT Access Control Policy

1.	Title of policy/ programme/ framework being analysed **Access Control 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

End of Policy Document