North Hampshire
Clinical Commissioning Group

HS South, Central and West Commissioning Support Unit

IT Access Control 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:	Phill Wade, Head of Technology Management and Operations
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:	All NHS South, Central and West CSU staff

Document Control Sheet

Title	**IT Access Control Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Stuart Collier – Information Security Manager
Date Created	06.01.2014
Date Last Updated	14.12.2017

History			
Version	Date	Author(s)	Comments
0.1	06.01.2014	Stuart Collier	Draft
1.0	08.01.2016	Phill Wade	SCW CSU Updates and version reset
1.1a	06.09.2016	Arif Gulzar	Updated policy review date and sections 4.5,5.2,5.4,5.5,6 & 9
1.1b	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**
Catherine Dampney	CIO

Phil Evans	Associate Director of IT Services

Contents

1 Introduction

This document defines the Access Control Policy for NHS South, Central and West Commissioning Support Unit (the CSU). 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 CSU.

Access Control policy is a key component of the CSU overall information security management framework and this policy should be read in conjunction with other CSU'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 CSU as set out in the security statement in the ISMS

2 Objectives

The objective of this policy is to prevent unauthorised access to the CSU, 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

This Policy covers all devices owned by or connected to the CSU 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
IGT	Information Governance 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 internet policy and other related information security policies are based is as follows;

- Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2001, 2008, 2010
- Access to Records Act 1990
- Common Law Duty of Confidentiality
- Fraud Act 2006
- Bribery Act 2010

4 Roles and Responsibilities

4.1 Accountable Officer

The Managing Director as the Accountable Officer has overall responsibility for Information Governance within the CSU. The post holder is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

4.2 Senior Information Risk Owner (SIRO)

The role of Senior Information Risk Owner (SIRO) in the CSU has been assigned to the Director of Corporate Development & Performance. The SIRO will be accountable for ensuring that information risks to the CSU and its customers are identified and managed in accordance with the Information Security Policies. This includes oversight of the CSU's information risk, security incident reporting and response arrangements.

4.3 Caldicott Guardian

The Caldicott Guardians have strategic roles which involve representing and championing Information Governance requirements and issues at executive team level and where appropriate, at a range of levels within the organisation's overall governance framework.

For the CSU, this will be the CSU Director of Operations with a portfolio which includes information. The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

4.4 Information Governance Service Lead

The Head of Information Governance has been appointed to act as the overall Information Governance lead for the CSU and under the approved arrangements.

The Head of Information Governance will be responsible for ensuring all tasks are undertaken in order to meet the required standards.

4.5 Cyber Security Manager

Responsibilities of the Cyber Security Manager will 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 the CSU.
- 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.

4.6 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are senior members of staff (Service Leads) responsible for information risks within their service areas and they are responsible for providing assurance to the SIRO that information risks and recorded and that controls are in place to mitigate those risks. IAOs will work closely with the CSU IG team and Information Security Manager to ensure that:

- Security of the Network used by their staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Their staff are made aware of their security responsibilities.
- Their staff have had suitable security training.
- An action plan and action outcome is developed in the event of a breach to the CSU Networks.

4.7 Data Custodians

IAOs can appoint a Data Custodian to support the delivery of information risk management responsibilities within their service areas. Data Custodians should ensure that:

- Staff within their areas aware of the CSU's policies and procedures and their responsibilities for the secure use of the CSU IT systems.
- They recognise actual or potential security incidents and take steps to mitigate those risks.
- They consult with their IAOs on incident management and ensure that information asset registers are accurate and up to date.

4.8 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 the CSU 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 the CSU 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 CSU Authoriser.

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 CSU 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 CSU 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 CSU'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 CSU 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 CSU'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 CSU IG and IT Services teams.

8 Dissemination and Implementation

This policy will be published on the CSU 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 NHS South, Central and West CSU 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 CSU'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
- Network Security Policy
- Business Continuity Plans