North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

IT Services - Network Security 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:	Matthew Rawles, Head of IT Enterprise Architecture & Design
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 &West CSU staff and Customers

Document Control Sheet

Title	**IT Services - Network Security Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Matthew Rawles
Date Created	18/06/2013
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
0.1	18/01/2016	Matthew Rawles	Initial SCW draft based on Stuart Collier's South CSU heritage document
0.1	27/01/2016		Approved by SCW Corporate Governance Assurance Group
1.0	03/02/2016	Matthew Rawles	Updated following comments from SCW Information Governance Group and approval from SCW Corporate Governance Assurance Group
1.1	08/09/2016	Arif Gulzar	Updated the Policy review date
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
Phil Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1 Introduction

This document defines the Network Security Policy for NHS South, Central and West Commissioning Support Unit (the CSU). The Policy applies to all staff working directly for the CSU, and any organisation that has entered into an agreement for the provision of IT services by the CSU.

The policy applies to all business functions and information contained on the Network, the physical environment and relevant people who support the Network. The Network is a collection of communication equipment such as servers, computers, printers, and modems. The Network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

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.

2 Scope and Aim

NHS South, Central and West CSU is committed to developing effective policies, procedures and other corporate documents that deliver compliance with our necessary governance requirements including expectations of our host body, our customers and external assessment organisations. While NHS South, Central and West CSU is hosted by the NHS Commissioning Board (NHS England), we will not develop or encourage arrangements that conflict with existing NHS England policies.

This policy applies to all Networks used for:

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images on behalf of the CSU customers e.g. continuing Health Care (CHC).
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

The aim of this policy is to ensure the security of the CSU Network and to do this, the organisation will:

- Ensure the protection of Network from unauthorised disclosure and accidental modification.
- Ensure the accuracy and completeness of the organisation's IT assets

3 Definition of Terms Used

CD-ROM	Compact Disc Read-only Memory
CRAMM	CCTA Risk Analysis and Management Method
IT	Information 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

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. The SIRO will identify and manage the information risks to the CSU and with its partners. 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 Information Security Manager

Responsibilities of the Information Security Manager will include:

- Acting as a central point of contact on information 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 information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information 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.

5 Policy Detail

5.1 Risk Assessment

- Risk assessment will be conducted on the network annually, the scope of the risk assessment will changed depending on which area of the network needs to be assessed
- Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the Network.
- Formal risk assessments will be conducted using CRAMM methodologies and will conform to ISO27001 standards.

5.2 Physical and Environment Security

- Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive Network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.
- All public network facing firewalls will be accredited to EAL4 as a minimum.
- Areas which are controlled with secure key-code locks will be periodically changed, following a compromise of code or when a member of staff leaves.
- Critical or sensitive Network equipment will be protected from power supply failures.
- Critical or sensitive Network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive Network equipment.
- All visitors to secure Network areas must be authorised by a senior member of the IT department.
- All visitors to secure Network areas must be made aware of Network security requirements.
- All visitors to secure Network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

  The Information Security Manager will ensure that all relevant staff is made aware of procedures for visitors and that visitors are escorted, when necessary.

6 Access Controls

6.1 Access to Secure Network Areas – CSU Staff

The CSU will ensure that:

- Access to secure network areas is restricted to staff who require access to the area
- Accesses to secure areas are regularly reviewed and ensure that the list is accurate and up to date.

6.2 Logical Access to Network – All NHS Staff

- All access to the network must be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- a formal registration and de-registration procedure is followed to control access the network and systems, with appropriate line manager authorisation.
- Access rights to the network must be allocated based on the user's role rather than user's status within the organisation.
- User access rights will be removed or reviewed when a user leaves the organisation or changes job.

- All users must have an individual user identification (username) and password.
- Users are responsible for ensuring that their username and password is kept safe.
- Generic/shared user identification and password will only be granted with a justifiable business requirement and must be only used for the purpose they have been created for.
- All users must conform to the Acceptable Use Policy.

6.3 Third Party Access to the Network

- Third party access to the network will based on a formal contract that satisfies all necessary NHS Security conditions
- All third party accesses to the network will be managed and logged.

6.4 Connections to External Networks

- Ensure that all connections to external networks and systems have documented and approved System Security Policies.
- Ensure that all connections to external network and systems conform to the NHS-wide Network Security policy, Code of Connection and supporting guidance

6.5 Access via VPN (Virtual Private Network) – All NHS Staff

- Ensure that all connections to external networks and systems have documented and approved System Security Policies.
- Ensure that all connections to external network and systems conform to the NHS-wide Network Security policy, Code of Connection and supporting guidance
- All access via VPN must authorised by the user's line management using the appropriate documentation.
- All users must conform to the Remote Access Policy

6.6 Wireless Network Access

Access to the network wirelessly will also be in accordance with the requirement of this policy. There will also be additional access controls via certificate and radius servers.

7 Operating Procedures

7.1 Data Backup and Restoration

The Information Security Manager is responsible for ensuring that:

- Backup copies of Network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes are produced and communicated to all relevant staff.
- Backup tapes are stored securely and copies stored off-site.
- There are documented procedures for the safe and secure disposal of IT equipment including backup media and these procedures are communicated to all relevant staff.
- The disposal of backup media follows and complies with the CSU policy for decommissioning and disposal of old equipment.

7.2 Fault Logging

The Information Security Manager will ensure that a log of all faults on the Network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

7.3 Business Continuity

The CSU will ensure that:

- There are existing Business Continuity and Disaster Recovery Plans for all critical systems.
- The Business Continuity Plans and Disaster Recovery Plans are regularly reviewed and the process is tested annually.
- The plans must be reviewed by the IAO and tested on a regular annually

7.4 Accreditation of Network Systems

Ensure that the Network is approved by the IT Services Senior Manager of Network Operations before it commences operation; ensuring that the Network does not pose an unacceptable security risk to the organisation and meets Information Governance Toolkit (IGT) requirements/standards.

7.5 System Change Control

The Head of Technology Management and Operations will ensure that:

- changes to the security of the Network are in line with the CSU Change Control procedures.
- Relevant Network Security Policies, design documentation, security operating procedures and Network operating procedures are updated regularly especially when changes to legislations or national guidance necessitates an early review.
- Acceptance testing of all new Network systems is be carried out, in line with Information Security requirements.

Any changes to network configuration must go through the CSU Change Control Procedure

Testing facilities will be used for all new Network systems. Development and operational facilities will be separated.

7.6 Maintenance Contracts

The Head of IT Strategy and Planning will ensure that maintenance contracts are maintained and periodically reviewed for all Network equipment. All contract details should constitute part of IT Asset register

8 Incident – Reporting, Investigations and Resolutions

All staff should ensure that they report actual/potential security incidents as soon as they become aware to their Data Custodian. In the absence Data Custodian actual/potential security incidents should be reported the IAO or the CSU IT service desk.

All incidents, investigations and resolutions will be recorded on the Service Desk system for reporting, knowledge base and future learning.

There may be instances where incidents are reported directly to the Security team or Information Governance due to their sensitivity. These are likely to be legal and/or forensic incidents which will be dealt with according to the CSU Incident Management and Reporting Procedures.

8.1 Monitoring and Audit

In order to provide assurances that controls in place are working effectively, the Information Security Manager will work closely with the CSU IG team to ensure that audits of systems and access controls to networks are conduct on a regular basis. Examples of events that will be audited will include frequency, circumstances and location etc.

- Failed attempts to access confidential information
- Repeated attempt to access confidential information
- Shared login and passwords

The CSU will ensure that:

- There is continuous improvement in confidentiality and data protection and learning outcomes;
- All incidents are audited to ensure any recommendations made have been implemented.
- An action plan and action outcome is developed in the event of a breach to the CSU Networks.
- Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring;

  This will ensure that the CSU fully embeds improvements to its information governance structure and demonstrate it is proactive in assessing and preventing information risk.

9 Policy Review

In line with the CSU's key documents, this document 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.

10 Dissemination and Implementation

This document will be published on the CSU intranet. IAOs and other senior 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 ICT services by the South CSU should ensure that this document and other IT related documents are cascaded to their staff.

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 team.

11 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
- Information Security Incident Management and Reporting Procedures
- Access Control Policy
- Business Continuity Plans

12 Equality, Diversity and Mental Capacity

NHS South, Central and West CSU recognises the diversity of the local community and those in its employment. The organisations aim to provide a safe environment free from discrimination and, a place where all individuals are treated fairly, with dignity and appropriately to their need.

This document was assessed against the NHS South, Central and West CSU Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time.

This document has been assessed and meets the requirements of the Mental Capacity Act 2005.