Network Security Policy Version 3

South, Central and West Commissioning Support Unit

July 2018

Version Number: 3	Issue/approval date: 24 July 2018
Status: Final	Next review date: July 2019

DOCUMENT CONTROL

Document Name	Version	Status	Author
Network Security Policy	*3.0*	*Final*	*Associate Director of Technology Management & Architecture*
Document objectives:	*The objective of this Policy is to safeguard the confidentiality, integrity and availability of information, information systems, applications hosted or managed within SCW networks from internal or external threats.*		
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: 24 July 2018*	
Date issued:	*24 July 2018*		
Review date:	***July 2019***		
Author:	*Associate Director of Technology Management & Architecture*		
Lead Director:	*Director of IT Services*		

Version Control

Date	Author	Version	Page	Reason for Change
18/01/2016	Matthew Rawles	0.1		Initial SCW draft based on Stuart Collier's South SCW heritage document
27/01/2016		0.1		Approved by SCW Corporate Governance Assurance Group
03/02/2016	Matthew Rawles	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 the Policy review date
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
17/05/2018	Arif Gulzar	2.2	All	Updated corporate policy template with corporate branding. Updated section 3 definitions Updated section 4 with roles and responsibilities Updated section 5 with Cyber essentials plus standard Added Technical Consultant (Cyber) role to 5.2 Some minor changes to sections 6.2,6.5, 7, 7.2,7.4,7.5, 7.6, 8 and 8.1
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

Version Number: 3	Issue/approval date: 24 July 2018
Status: Final	Next review date: July 2019

CONTENTS

1 Introduction 5

2 Scope and Aim 5

3 Definition of Terms Used 6

4 Policy Detail 6

5 Access Controls 7

6 Incident – Reporting, Investigations and Resolutions 10

7 Roles and Responsibilities 11

8 Monitoring and Audit 13

9 Policy Review 13

10 Dissemination and Implementation 14

11 Related Documents Policies and Procedures 14

APPENDIX A - Equality Impact Analysis 15

1 INTRODUCTION

This document defines the Network Security Policy for SCW. The Policy applies to all staff working directly for the SCW, and any organisation that has entered into an agreement for the provision of IT services by the SCW.
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.

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

SCW 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 SCW 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 SCW customers, for example, 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 SCW 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
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 Owner

4 POLICY DETAIL

4.1 RISK ASSESSMENT

- SCW is responsible for ensuring that appropriate risk assessment(s) are carried out in relation to all the business processes covered by this policy. The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability
- Risk assessment(s) will be conducted on the network annually as part of cyber essentials plus accreditation, the scope of the risk assessment(s) will depend on which area of the network needs to be assessed

- Risk assessment will be conducted to determine the compliance with cyber essentials plus standard as per Data Security and Protection toolkit to test the effectiveness of security controls that protect the network

4.2 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 Cyber Security Manager and Cyber Security Technical Consultant will ensure that all relevant staff is made aware of procedures for visitors and that visitors are escorted, when necessary

5 ACCESS CONTROLS

5.1 ACCESS TO SECURE NETWORK AREAS – SCW STAFF

SCW 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

5.2 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 user 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. The accounts MUST comply with SCW password policy
- All users must conform to the Acceptable Use Policy & Information security policy

5.3 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

5.4 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

5.5 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, HSCNConnection agreement 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 Working and Portable Device Policy

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 Operating Procedures

5.6 DATA BACKUP AND RESTORATION

The Technical consultant (Cyber) 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 SCW policy for decommissioning and disposal of old equipment

5.7 FAULT LOGGING

The Technical consultant (Cyber) 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.

5.8 BUSINESS CONTINUITY

The SCW 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 annual basis

5.9 ACCREDITATION OF NETWORK SYSTEMS

Ensure that the Network is approved by the Enterprise Architect before it commences operation; ensuring that the Network does not pose an unacceptable security risk to the organisation and meets Data security and protect toolkit requirements/standards including HSCN connection agreement.

5.10 SYSTEM CHANGE CONTROL

The Associate Director of Technology Management and Architecture will ensure that:

- Changes to the security of the Network are in line with the SCW 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 to be carried out, in line with Information Security requirements
- Any changes to network configuration(s) must go through the SCW Change Control Process
- Testing facilities will be used for all new Network systems. Development and operational facilities will be separated

5.11 MAINTENANCE CONTRACTS

The Associate Director of Technology Management and Architecture will ensure that maintenance contracts are maintained and periodically reviewed for all Network equipment. All contract details should constitute part of IT Asset register and IT contracts database.

6 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 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 Cyber Security team or Information Governance due to their sensitivity using SCW incident management system (DATIX). These are likely to be legal and/or forensic incidents which will be dealt with according to the SCW Incident Management and Reporting Procedures.

7 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 the 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 the 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.

8 MONITORING AND AUDIT

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

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

SCW will ensure that:

- There is continuous improvement in complying with the common law duty of confidentiality and data protection legislation 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 SCW Networks
- Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring;

This will ensure that the SCW 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 SCW'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.

Version Number: 3	Issue/approval date: 24 July 2018
Status: Final	Next review date: July 2019

10 DISSEMINATION AND IMPLEMENTATION

This document will be published on the SCW intranet. Information Asset Owners 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 IT services by the SCW 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 SCW IG team.

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

APPENDIX A - EQUALITY IMPACT ANALYSIS

On Network Security Policy

1 What is it about? ***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Confidentiality and Safe Haven Policy details how SCW will meet its legal obligations and NHS requirements concerning confidentiality, information security standards and operates such procedures ensuring that confidential information sent to or from SCW is handled in such a way as to minimise the risk of inappropriate access or disclosure. For the purposes of this policy, where Personal or Special Categories of Data are described this will include data that is owed a duty of confidentiality under the Common Law.
b) Who is it for? All staff
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the confidentiality of information to be of equal status across all groups of people.
d) What are the barriers to meeting this potential? There are no barriers.
2 Who is using it? ***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy.
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.
3 Impact ***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? This is not applicable.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.

d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Simon Sturgeon**	Date completed: **24-07-2018** Proposed EIA review date: **01-07-2019**
Signature of director/decision-maker **Simon Sturgeon** Name of director/decision-maker **Simon Sturgeon**	Date signed **24-07-2018**