NHS
North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

IT Services Security Framework

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.

Version:	2.1
Ratified by:	SCW CSU Corporate Governance Assurance Group
Date ratified:	29/11/2016
Name of Responsible Officer/author:	Andy Ferrari – Associate Director of IT Strategy and Planning
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 Services Security Framework**
Version	2.1
Status	Approved – Final
Author	Andy Ferrari
Date Created	19/01/2016
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
0.1	19/01/2016	Andy Ferrari	Initial SCW draft based on Stuart Collier's South CSU heritage document
1.0	02/02/2016	Andy Ferrari	Finalised - Updated following comments from SCW Information Governance Group and approval from SCW Corporate Governance Assurance Group
1.1a	08/09/2016	Arif Gulzar	Updated the policy review date and some minor changes
1.1b	04/10/2016	Arif Gulzar	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 framework review date to align with GDPR after approval from SCW Information Governance Steering Group

Approval/Sign Off	
Name	**Title and contact**
Philip Evans	Associate Director of IT Services
Catherine Dampney	CIO

Contents

1. Introduction

1.1 Information is an important asset and of significant value to NHS South, Central and West Commissioning Support Unit (CSU) and its customers. At the same time as providing access to information, we must also protect it from threats, internal and external. Deliberate or accidental, that could disrupt it our work or infringe the rights and confidentiality of our staff and customers.

1.2 Information management are the processes about how we create, obtain, distribute, destroy (or archive) and provide information.

1.3 Information security involves the protection of information for **Confidentiality, Integrity and Availability.**

1.4 This document provides a high level explanation of the framework in use at NHS South, Central and West CSU to secure information assets.

2. Scope

This document applies to all information irrespective of format. This includes:

- All corporate information systems;
- All paper records;
- Visual and photographic materials e.g. CCTV, slides
- Spoken conversation, including voicemail and recorded conversations; and the technology used to hold, process, transfer and transmit information e.g. memory sticks.

3. The Framework

3.1. NHS South, Central and West CSU continuously reviews and organises its information to adapt to legislative changes and changes to customer needs.

3.2. In common with accepted best practice, we employ a layered approach to information security. We protect Information inside a hierarchy of physical, technical and procedural measures

3.2.1 Physical Security Layer. All information assets are physically located in secure accommodation. Electronic information is generally stored on servers located in a secure, air-conditioned and fire-protected room. Staff process information in access-controlled offices while paper-based information is stored in lockable storage. Most offices are protected by door access systems. Staff working from home or from remote locations must be provided with appropriate physical security measures. Partners and 3rd parties working as agents of NHS South, Central and West CSU must provide the same level of protection for our information.

3.2.2 Logical and Technical Layer. Controlling access to information and protecting it from a wide range of threats is the job of the logical and technical layer. User accounts, access tokens, antivirus and backup systems are all examples of the measures NHS South, Central and West CSU employs to protect the confidentiality, integrity and availability of its information.

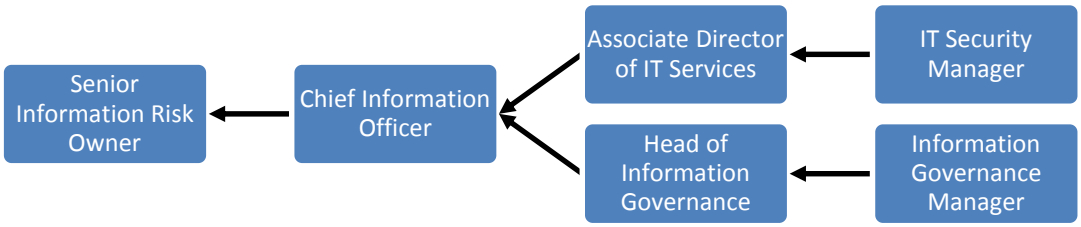
3.2.3 Administrative Layer. Often regarded as the most important, the administrative layer is about people, organisational policies, training and security awareness. It is no accident that the framework model shows this as the innermost security layer surrounding our information. All the physical and technical protective measures possible would be completely ineffective if, for example, a user allows their access credentials to fall into the wrong hands.

3.3. Policies and procedures must be robust and must be backed up by an effective training and security awareness programme. In addition to reading and signing for the Information Security Policy and supporting policy documents, all staff must complete an online Information Governance training course.

4. Security Statements

- NHS South, Central and West CSU consider its own, and customers, information one of its most valuable assets.
- NHS South, Central and West CSU will protect the confidentiality, integrity and availability of all information in its possession.
- NHS South, Central and West CSU will continue to develop effective methods of making its information securely available.
- NHS South, Central and West CSU will maintain an information management and security framework that is “fit for purpose”.
- NHS South, Central and West CSU will make sure all staff receive regular and effective information security and awareness training.
- NHS South, Central and West CSU will make available to customers senior management, when requested, reports on the current Information Security standing.
- NHS South, Central and West CSU will maintain a corporate risk register which will contain reference to Information Security (when applicable)

5. Roles and Escalation



6. Information Security Reporting

All information security related calls should be logged with the NHS South, Central and West CSU Service Desk.