North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

Information Security Assurance Plan

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:	1.1
Ratified by:	Information Governance Steering Group
Date ratified:	14.12.2017
Name of Responsible Officer/author:	Arif Gulzar – Cyber Security Manager
Name of responsible committee/individual:	IT Strategy and Planning Group
Date issued:	09.01.2018
Review date:	25.05.2018

Document Control Sheet

Title	IT Services – Information Security Assurance Plan
Version	1.1
Status	Approved – Final
Author	Arif Gulzar
Date Created	01.03.2016
Date Last Updated	14.12.2017

History			
0.1	01.03.2016	Arif Gulzar	Draft based on the heritage document
0.2	04.10.2016	Arif Gulzar	Final review prior to sign off
1.0	10.11.2016	Arif Gulzar	Version reset after approval from IG Steering Group
1.1	14.12.2017	Arif Gulzar	Extended plan review date to align with GDPR after approval from SCW Information Governance Steering Group

Contact Details		
Arif Gulzar	0758 427 6282	arif.gulzar@nhs.net

Approval/Sign Off		
Version	**Approving Committee**	**Date Approved**
1.0	Information Governance Steering Group	10.11.2016
1.1	Information Governance Steering Group	14.12.2017

1.1 Overview

NHS South, Central and West Commissioning Support Unit (SCW) uses several mechanisms to manage Information Security (IS) aligned with the International Information Security Standard - ISO27001. These are detailed below and in the relevant written controls.

1.2 Management of Information Risk

In order to appropriately manage Information Risk and prioritise the Information Security Assurance Plan, it is important to identify and quantify risk through the routine work of the SCW IT services. This risk needs to account for the value of the asset, the potential severity of any impact and the likelihood of an occurrence. It is undertaken in line with the Risk and Assurance framework(s) for the organisation.

The IT Security Manager maintains a list of IT Security issues, risks and mitigations for routine discussion with the relevant SIRO. This includes information that is held on-site and within current networks, as well as that held off-site and off-line, including appropriate disposal and destruction processes to the required standard.

Risks are captured on the SCW IT Services Risk Register and are reviewed on a regular basis, with inclusion on the overall Corporate Risk Register where required. These are reviewed on a regular basis in accordance with the organisation's Risk Management Policy and Strategy.

Responsibility for managing Information Security within the SCW / CCG rests with all employees and the following key officers:

- SIRO (Senior Information Risk Owner)
- Chief Information Officer
- IT Security Manager* / Information Governance Manager
- Information Asset Owners (IAOs)

(*) SCW have a dedicated IT Security Manager with overall responsibility for IT Security guidance, policies and processes.

The ISO27001 methodology of Plan-Do-Check-Act ensures that all areas of Information Security are under regular and controlled review.

1.3 Information Security Policies

Appendix 1 lists the current policy control set which forms the Information Security Management System (ISMS) for SCW and are aligned to the requirements for ISO27001.

All Information security policies are reviewed annually, and published on the SCW intranet.

1.4 System Level Security Policies

Each IT services key information system (Asset) is required to have a system level security policy that details, where appropriate:

- Access control requirement specifications (such as whether two factor authentication is required and is in place)
- Authorisation process for access to the system (user registration and deregistration)
- Assignment of responsibilities for the system (access, maintain and issue resolution)
- Details on system design and dependencies
- Provisions for audit reports generated by system utilities
- Detail on system documentation in place
- Access controls (e.g. password strength and threshold of failed logins)
- Backup requirements
- Back-up data testing arrangements
- Business Continuity or Back-up plans for system data and software applications

The policy must detail what security reports are available and who can provide them for the following issues, where appropriate:

- Access log files generated by the system
- Current User overview
- Account Monitoring (e.g. unused accounts, unauthorized access)

The system level policy will be reviewed on an annual basis, or following significant changes to the system.

1.4.1 Definition of a Key Information System (Asset) Key Information Systems (Assets) are defined as:

- *Systems which other business critical assets are dependent upon (e.g. Network)*
- *Business Critical*

1.5 Information Security Incidents

Any IT Security Incidents will be recorded and reported to the SIRO on a routine basis. The report will note which issues were resolved, which have been escalated as risks and the associated action plan for the management or mitigation of the risk.

1.6 Information Sharing and Transmission

Where information is shared or transmitted, maintaining the security, confidentiality and integrity of the data is a requirement of the organisation's legal obligations. This is in addition to ensuring an appropriate lawful basis. No Personal Confidential Data will be shared, transmitted or published without the appropriate approval of the organisation or reference to the relevant process, such as legal disclosure or disclosure under Data Protection or Access to Health Care provisions.

1.7 Performance of Information Systems

The performance of Information systems and dependencies will be provided to the SIRO and Director with responsibility for IT Services, where applicable, on at least a quarterly basis. Any risks resulting from performance which impact the confidentiality, integrity or availability of systems and/or data will be added to the relevant Risk Register in line with the Risk Management Policy and Strategy.

Information Systems consist of, but are not limited to:

- Network(s)
- Servers
- Key databases and datasets
- Email systems
- Desktop / Laptop / Mobile devices

1.8 IT Security Testing and Evaluation

SCW undertake regular vulnerability assessments against hosted systems and services to minimise the risk of unauthorised access and subsequent data loss. External network access (e.g. Access from the internet) is assessed annually from a Check/Crest(*) accredited company.

IT Services is subject to the annual external Service Audit Reviews (SARs) carried out by Deloitte. In order to deliver assurance over the internal controls and control procedures operated by a service organisation to its customers and their auditors, many organisations engage a reporting accountant to prepare a report on internal controls. NHS England has chosen to follow this approach as the method of providing assurance to Clinical Commissioning Groups (CCGs) over the services provided by Commissioning Support Units (CSUs). The objective of this is to provide assurance in a cost effective manner for the NHS through reducing the duplication which would likely arise from multiple CCG internal and external auditors separately assessing SCW controls.

The IT Security Manager provides advice on new projects, and procurement of new services from inception to delivery to ensure IT Security has been addressed.

(*) Government approved contractor accredited to perform vulnerability assessments against public sector organisations.

1.9 Information Risk Owner Review

SCW IT Services are required to provide an annual update to the Senior Information Risk Owner on the management of information risks related to the information assets utilised within their remit. This includes a review of the controls and their effectiveness.

REGULATION AND LEGISLATION WE COMPLY WITH (ISO27001):

- **DATA PROTECTION ACT (UK) 1998**
- **COMPUTER MISUSE ACT 1990**
- **COMMUNICATIONS ACT 2003**
- **FREEDOM OF INFORMATION ACT 2000**
- **REGULATION OF INVESTIGATORY POWERS ACT 2000**
- **FRAUD ACT 2006**
- **BRIBERY ACT 2010**
- **COPYRIGHT, DESIGNS AND PATENTS ACT 1988**
- **WASTE ELECTRICAL AND ELECTRONIC EQUIPMENT (WEEE) REG. 2012**

LEGISLATION IS COVERED BY INDUCTION TRAINING AND ONGOING SECURITY TRAINING

Appendix 1 – Information Security Policies

The following published policies form part of the Information Security Management System (ISMS) aligned with ISO27001.

- IT Services - Acceptable Use Policy
- IT Services - Backup and Business Continuity Policy
- IT Services - Anti-Virus Policy
- IT Services - Clear Screen & Desk Policy
- IT Services - Service Equipment Disposal Policy

- IT Services - Information Security Policy
- IT Services - Network Security
- IT Services - Password Policy
- IT Services - Registration Authority Policy
- IT Services - Remote Working & Portable Devices Policy
- IT Services - Security Incident Handling Policy
- IT Services - Security Framework
- IT Services - System Level Security Policy
- IT Services - Access Control Policy
- IT Services - Change Management Policy
- IT Services - Core GPIT Service Provision Policy