North Hampshire
Clinical Commissioning Group

NHS South, Central and West Commissioning Support Unit

System Level 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:	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 System Level Security Policy**
CCG	All
Version	2.1
Status	Approved – Final
Author	Stuart Collier
Date Created	18/06/2013
Date Last Updated	14/12/2017

History			
Version	Date	Author(s)	Comments
0.1	18/06/2013	Stuart Collier	Draft
1.0	07/01/2016	Phill Wade	SCW CSU updates and version reset
1.1a	08/09/2016	Arif Gulzar	Updated policy review date, section 2 & 3
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 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

INTRODUCTION

The development, implementation and management of a system level security management procedure will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

An effective system level security management procedure will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of person identifiable / sensitive data.

Current encryption guidance for NHS organisations can be found at http://systems.hscic.gov.uk/infogov/security/infrasec/iststatements/dataenc_html. It would be expected that any electronic solution for the handling of person identifiable / sensitive data to comply with this guidance as a minimum.

In addition - NHS organisations are required to comply with the range of best security management practices as set out in ISO/IEC 27001:2013. The system level security management procedure is a core component of an accreditation documentation set for those organisations that undertake formal accreditation processes for their information assets.

Where the system is available to multiple organisations, the system level security management procedure must establish the necessary common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

The following series of topics are relevant for any system level security policy and are intended to help guide responsible staff through their considerations for the development of their system level security documentation. This list is not exclusive of all possibilities and it is the responsibility of each information asset owner to identify and consider their security management needs on a case by case basis. This is best achieved through a formal process of risk assessment and mitigation.

Implementation

The requirement for the completion of the SLSP will be captured at either

- The procurement stage of new or replacement systems

Or

- The Privacy Impact Assessment (PIA) review carried out by the NHS South, Central and West Commissioning Support Unit (CSU) Information Governance (IG) Team

Sign-off and recording of completed SLSPs will be undertaken by the SCW CSU IG Team.

Review

An annual review of recorded SLSP's will be undertaken by the IG team, with the assistance of CSU IT Services, to ensure the list is current and accurate. Significant changes to systems will require the SLSP to be reviewed and updated outside of the review cycle. The remaining sections provide the template for an SLSP and are aligned to the latest SLSP template available from the HSCIC website at the time of writing.

1. SYSTEM DETAILS:

The System shall be known as:	*[Insert full System Name]*
The System's responsible Information Asset Owner shall be: *[Insert details for the most senior member of staff accountable for the system i.e. Associate Director] (Note: this member of staff is the lead individual responsible for accrediting the system's security implementation)*	Name: Job Title: Department: Extension:
The System's responsible Information Asset Administrator/Data Custodian/Caldicott Guardian shall be: *[Insert details for the member of staff responsible for the day to day management of the system i.e. System Manager]*	Name: Job Title: Department: Extension:
The System's deputy information asset administrator shall be:	Name: Job Title: Department: Extension:
The Systems Data Controller shall be:	CSU or CCG
What information is held on the system e.g. Demographics, Clinical Details	
Is the System compatible with the NHS number?	*Yes/No*

2. SYSTEM SECURITY:

2.1 Security of the system shall be governed by the CSU's corporate information security policy and other associated policies and procedures.

2.2 The Data Custodian/Information Asset Administrator duties are shown at appendix (a).

2.3 The System shall incorporate the following security countermeasures:

Access Control: [logical security measures and privilege management]

Authentication Method: *[Please tick]* *Access control must be in place on all systems. Authentication should ideally be by username & password or two factor authentication.*	User Name & Password:		Two Factor (Smartcard)	
	Other (Please Specify)		Two Factor (Other – Please Specify)	
Password Complexity: *[Note: If any of this criteria is not met, please identify this as a risk in the system risk assessment]* *The minimum password complexity should be:* - *A minimum of 8 characters* - *Require a combination of at least letters and numbers and ideally symbols.* - *Require a mixture of UPPER and lower case characters.*	Maximum number of characters:		Minimum number of characters:	
	Minimum number of letters Required:		Minimum number of numbers Required:	
	Minimum number of lowercase characters required		Minimum number of uppercase characters required	
			Minimum number of symbols/special characters required:	
Password change period: Every….. *Systems should force users to change their passwords at least every 3 months.*				
Number of allowed password attempts before user account locked *Accounts should lock if a user enters an incorrect password 3 times. The user should then be required to contact a system administrator to re-activate their account (see un-lock procedure below).*				
If the system is accessed by username and password, does the system identify which element (i.e. username or password) that has been entered incorrectly? *(Yes/No)* *The system should not identify, which element has been entered incorrectly.*				

Un-lock Procedures: *(Please document how a user goes about retrieving their username/password if forgotten and/or unlocking their account)* *There should be a process in place to confirm the identity of the user prior to un-locking their account.*	

Inactivity time-out period: *Time out periods may vary considerably. Ideally the time-out period should be set to 10 minutes of inactivity.*	
Registration procedures: *[Note: Include procedures as an appendix if already established in a separate document. Please document any security/system training provided to users].* *All access provided should be authorised & users should be provided with appropriate system/security training.*	
Deregistration procedures: *[Please include a statement as to whether the IAA/DC has access to leavers reports from the Human Resources department and how access is changed or removed for staff changing roles within the CSU].* *Please also include procedures for any temporary access/accounts given i.e. whether a termination date is set.* *All system manager's/IAA's should use ESR reports to deactivate system accounts that are no longer required.* *System managers should ensure, where temporary accounts are used, that they are appropriately 'timed' and/or removed when no longer required.*	
Records of all users and access levels provided are retained by the IAO: *Yes/No* *Records of all users and access provided should be retained by the system manage IAO.*	
Please list all 'privileged users' of the system *i.e. users that can change core components of the system, including access levels, e.g. system administrators.* *Records of all users and access provided should be retained by the system manager IAO*	
Please identify the possible levels of access *a user can be given and list any significant user groups. This may be job role specific or by user group.* *Records of all users and access provided should be retained by the system manager/IAO*	

Physical Security Controls for Hardware e.g. Server/s, back-up tape drives etc.:

Access control and security should be applied to all server rooms. Other hardware such as back-up tapes should be stored safely and securely i.e. in a physically secure area and fire proof safe.

Secure Room Yes/No		Secure Cabinet Yes/No	
Other (Please Specify)			

Network Security Controls:

The network should be protected by appropriate technical measures, such as firewalls, intrusion detection etc.

Firewalls Yes/No		Network Segregation Yes/No	
Other (Please Specify)			

Additional Security Controls:

All contractors should provide assurance of their compliance with information security requirements and best practice, by means of completing the IGT for third parties or providing an ISO27001 accreditation certificate.

Penetration testing should be undertaken on the organisation's network at least annually. Individual servers may require a separate penetration test depending on the circumstances.

All systems should log and retain audit trails i.e. log on audits, access to records and modification of records. A random sample should be selected from these audit trails and the appropriate checks undertaken to ensure records/systems have been accessed appropriately.

Contractor/Supplier Certification arrangements	
Audit Trails (Please Specify e.g. Log on audit and whether/how this is checked/monitored)	
Security testing i.e. Independent Penetration Testing Frequency	
Other (Please Specify)	

3. SYSTEM MANAGEMENT:

Maintenance & Support:	
The System shall be developed / provided by: *[Insert provider full Name]* (Note: if the system is developed or provided under commercial contract, then the relevant contract schedules that bind the contractor to the lead organisation's corporate security policy and to this system level security policy should be referenced)	
The System shall be implemented by:	
The System shall be maintained by: [Please note under what arrangements include responsibility for relevant aspects of security configurations. Also, identify the conditions applicable for the repair / replacement / disposal of equipment or media that may contain person identifiable data]. Equipment must always be handled and destroyed securely. Where equipment is no longer required an appropriate certificate should be provided to evidence that equipment has been destroyed securely. An appropriate confidential agreement should be completed (signed by the IAO and the Contractor/Supplier) and included as an appendix. A risk assessment should be carried out prior to any proposed agreement with a third party, the risk assessment should as a minimum take into consideration the level of access and any use of sub-contractors.	

Remote Access Support Arrangements (if applicable): Please state whether the Contractor/Supplier requires remote access to the system and the arrangements in place to secure any personal data. Please state the method of access i.e. internet (web-ex), N3, Portwise, VPN. Please reference any Remote Access Support arrangements within the Contractor/Supplier confidentiality agreement. Please refer to the Remote Access and Mobile Working Policy.	
The System shall be shared or used by the following organisations: (Note: record all participating bodies (stating whether NHS or other) and their purposes - Where the system is shared across multiple legal entities it is essential to identify how this security procedure will apply to all parties and how its effect will be measurable). An appropriate information sharing protocol and information sharing agreement should be completed for each organisation.	

4. SYSTEM DESIGN:

Electronic Based Systems or Paper based system	
Describe the system and purpose.	
Describe the network that will house the system i.e. existing CSU, independent or cloud network?	
Does the system require the use of a dedicated/virtual/cloud file server? Please state.	
Does the data reside with the system software? Please state where the data resides i.e. server/ network drive / Cloud.	

State any links to any wider network clouds e.g. site LAN, Internet and / or any other external network	
State any firewalls / gateway control devices.	

5. OPERATIONAL PROCESSES:

Back-Up Procedures:	
Back-Up Routine: [Please identify the frequency back-up data is recorded. Please specify arrangements for both system data and software]. System data should be backed up at least on a daily basis. System software should be backed up at least weekly.	
Verification Routine: [Please identify and data validity tests undertaken].	
Shutdown/Restart Process:	
Dependencies: [Please identify any interfaces the system has in place e.g. to PAS].	
Testing: [Please identify the frequency of tests, whether test data is used, whether tested in a simulated live environment and by what means the test is undertake, for example simulations/walk through exercises]. *Back-ups and recovery plans should be tested regularly (at least annually). Table top exercises should be undertaken using test data in a simulated live environment i.e. using back-up servers.*	

Data Collection Activities:	
The person identifiable / sensitive data will be collected by: [Please Tick].	
Directly from the Data Subject e.g. the patient is present when providing the information and the information is directly input on the system.	

On-line means i.e. Internet/Intranet/Email: [Please indicate security arrangements e.g. SSL VPN and encryption standards]. Encryption must meet approved NHS standards i.e. 256 bit strength.	
Paperwork**:** [Please indicate security arrangements e.g. follow-up arrangements to identify lost post for posted paperwork]. Safe Haven procedures must be followed. Please see the Information Sharing & Safe Haven Policy.	
Data on CD: [Please indicate security arrangements e.g. encryption standards]. Encryption must meet approved NHS standards i.e. 256 bit strength.	

Storage Arrangements:

The data will be stored: [Please Tick] For How Long?	
In what format (paper or electronic), where will it be stored & under what security controls?	
Any anonymisation process for person identifiable / sensitive data will need to be described. Please state whether data is pseudonymised for all secondary purposes? If not please identify which secondary purposes use identifiable information.	
How (and under what security controls) will person identifiable / sensitive data be loaded onto any file server / storage device.	

Encryption standards should be employed for stored data. (Note: any device not in a secure area that will cache or store person identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container. Backup copies of person identifiable / sensitive data also need to be encrypted).

Note: for added risk protection staff are encouraged to encrypt person identifiable / sensitive data stored on devices located in secure areas. Although not an NHS requirement, it may be prudent that such a step is taken should it be perceived a possibility of equipment loss or other attack.

Processing Arrangements:	
The data will be processed: [Please Tick]	
Paper Based Systems: [Please describe the data handling process (referencing any flowchart at the end of the system level security management procedure).	
Electronic Based Systems:	
List the user devices (desktop, laptop, PDA, iPAD etc.) that will access and process the data.	
State whether any of these devices will cache or store any of the data. If so, indicate the encryption standards to be employed. (Note: any device not in a secure area that will cache or store person identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container).	
State whether remote access (over the Internet or otherwise) will be employed to access the data.	
Describe measures in place to prevent the interception of transmitted data (E.g. standalone network, encrypted path, etc.).	
Include any policy to prevent (or at the very least severely restrict) the copying of person identifiable / sensitive data to removable media.	
If applicable, include any policy to prevent the printing of person identifiable / sensitive data.	

Peripherals:				
Sufficient stock of any hardware required for the system is available at all times i.e. Smartcards / digital microphones. Please detail all available stock.				
Any spare stock is stored securely	Secure Room Yes/No		Secure Cabinet Yes/No	
	Other (Please Specify)			

Disposal Arrangements:	
When the system or its data has completed its purpose / has become redundant or is no longer needed, what methods will be adopted to dispose of equipment, back-up media or other stored data:	
(Note: that operating system provided utilities such as 'erase' may not destroy unwanted data – it is therefore desirable to employ a commercial strength data shredder or equivalent to prevent unauthorised disclosure of person identifiable / sensitive data).	

6. SYSTEM AUDIT:

6.1. The System shall be risk assessed every 12 months by applying the CSU's risk assessment method.

6.2. A risk management / security improvement plan shall be established to address all unacceptable risks.

Note:

i) Remember to take account of cross-boundary risk / dependency issues where the system is part of a larger service or multiple organisation arrangement.

ii) A summary of this review should be reviewed at the information security group meeting

It is incumbent on the applicant to notify the information security group of any proposed material change to the agreed system level security management procedure, so that any additional security review can be carried out.

Audit Arrangements:
The System shall benefit from the following internal / external audit arrangements (Please list all arrangements).

7. SYSTEM PROTECTION:

Business Continuity Plans:	
Business impact Review: *[Briefly explain/analyse the effect that a disruption might have upon your/the CSU's business function].*	
Disaster recovery arrangements: [Explain what resilience / contingency arrangements the system benefits from e.g. uninterrupted power supply (UPS)]. (Note: identify any separate plans and status).	
Planning: In the event of serious disruption or total system failure, business continuity shall be provided by the following means:	
Confidentiality: In the event of a security or confidentiality breach occurring the following procedure shall be followed:	

Malicious Code / Unauthorised Mobile Code:	
What controls and procedures are in place to protect against malicious code and unauthorised mobile code i.e. anti-virus software [Please specify the software name]	
Does the system support security updates to the server operating system? Yes/No	

Appendix (a) – Role & Responsibilities of the Information Asset owner

Statement of Acceptance of the role of Information Asset Owner

I agree to work to the principle roles and responsibilities as outlined below, as part of my information system management and administration duties, in the capacity of Information Asset Owner (IAO):

- To identify all their Information assets and maintain a register of these assets, ensuring that they are accurate and up to date.
- To undertake risk assessment for all their information assets, which includes the identification, review and prioritisation of perceived risks and implementing actions agreed to mitigate those risks.
- Support the Senior Information Risk Owner (SIRO) in the overall information risk management function, and to maintain their awareness of the risks to all their Information Assets.
- Ensure that staff and relevant others are aware of and comply with expected Information Security working practices for the effective use of their Information Assets. This includes records of the information disclosed from an asset where this is permitted.
- To ensure that appropriate business continuity and disaster recovery arrangements are established and maintained for each of their information asset.
- The review and implementation all information security related policies and procedures.
- To support the progress in programmes to achieve compliance/certification with ISO27001.
- The review and monitoring of security incidents affecting their information asset, their cause, resolution and future prevention.
- Undertaking and reviewing information security risk assessments and improvement plans for their information assets.
- To ensure that a Privacy Impact Assessment (PIA) is undertaken for all new systems and changes to existing systems or processes, which involve personal or sensitive data.
- Monitoring and auditing compliance of their information asset and their use in accordance with relevant security standards and policies.
- Receiving and reviewing information security related reports (e.g. internal audit) and ensuring that any recommendations or actions relating to their asset are implemented.
- Reviewing and commenting upon the security impact of information system development.
- Reviewing and implementing the information security requirements of the annual IG toolkit submission for their information assets
- Support the implementation of Information security related projects which may affect their information assets.
- Ensure that there is an effective process for authorising access to their information assets and for removing user access promptly.
- Ensure that there is an effective process for granting the appropriate level of access to authorised users of their information asset.

- Communicate information to their Business Group/Department/Team and Peers and take any agreed actions forward for implementation.
- Complete appropriate Information Governance training via the on-line Information Governance Training Tool (IGTT) and undertake any other systems specific security training, as necessary.
- Attend the information security group meetings and have familiarised themselves with all papers on the agenda. Arrange for, and inform the Group of their nominated deputies, for attendance and representation of the appropriate area(s) if they are unable to attend themselves.
- Observe professional and contractual standards of confidentiality at all times.

If at any point I no longer believe it is appropriate for me to be an Information Asset Owner, I will notify the SIRO immediately.

If I have any queries or concerns with regards to my responsibilities as an IAO I will contact the Head of Information Governance.

Name (Print)……

Job Title……

Team/Service……..

Organisation……

Signature…… **Date**……

Office Use Only:

Date received: …….

Received By: ……..