Bolton Clinical Commissioning Group

System Level Security Procedure

Policy Number	**IG017**
Target Audience	**CCG**
Approving Committee	**CCG Chief Officer**
Date Approved	**December 2019**
Last Review Date	**October 2019**
Next Review Date	**October 2021**
Policy Author	**IG Team**
Version Number	**V2.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	May 2017	IG Team	Progress to IM&T Operations Board for Approval
0.2	June 2017	IG Team	Amendments made following comments from IM&T Operations Board
1.0	December 2017	CCG Chief Officer	Approved as a Procedure.
1.1	September 2019	IG Team	Reviewed and updated, change of layout to Appendix
2.0	October 2019	IG Board	Approved
2.1	December 2019	CCG Chief Officer	Approved

Contents

1. Introduction

1.1. Background

The development, implementation and management of a system level security procedure (SLSP) 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 / special categories of data.

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 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 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.

This system level security procedure is 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.

1.2. Implementation

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

- The procurement stage of new or replacement systems; Or
- The Data Protection Impact Assessment (DPIA) review carried out Information Governance (IG) Manager

Completed SLSPs should be sent to the IM&T Operations Board for review and approval. Where systems contain personal data the SLSP should also be sent to the IG Board for review and approval.

The template for an SLSP is provided at Appendix 1; this is aligned to the latest SLSP template available from the NHS Digital website at the time of writing.

1.3. Roles and Responsibilities

All staff responsible for the development / introduction of new IT systems or where a requirement for a SLSP has been identified by a DPIA should adhere to this policy.

The System's responsible security manager is will be the Head of IT and the Cyber Security Lead

The Security Managers duties shall include:

- Security Sign off for system implementation;
- Raise and maintain security awareness;
- Conducting Confidentiality audits on the system;
- Review Information Asset risk assessments;
- Security Assurance for system decommissioning.

The Information Asset Owner (IAO) is accountable for:

- The secure use of the system;
- Recording and Maintaining the relevant information flows of personal data via the Data Flow Mapping register;
- Identifying and managing all Information Risks for this asset;
- Maintaining this Procedure on a regular basis at least annually.

This System Level Security Procedure shall be the responsibility of the Information Asset Owner and reviewed on an annual basis or sooner if substantive change occurs with the asset.

The Information Asset Manager (IAM) and Administrator (IAA) are responsible for maintaining the system in accordance with this procedure.

1.4. Monitoring the Effectiveness of the Procedure

An annual review of recorded SLSP's will be undertaken by the CCG's IT Department, with the assistance from the CCG's IT Provider, Bolton NHS Foundation Trust, 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.

1.5. Review

The Head of IT and the Cyber Security Lead along with the Information Governance Manager will review the procedure as per the review date, or in accordance with legislative and / or good practice changes.

Appendix 1: System Level Security Procedure Template

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 e.g. 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 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 System's Data Controller shall be:	*<Insert Details>*
What information is held on the system: *e.g. Demographics, Clinical Details*	
Is the System recorded on the relevant Information Asset Register:	*Yes / No (delete as appropriate)*
Flows of personal identifiable / special categories of data relevant and recorded and maintained in the Data Flow Mapping Register:	*Yes / No Flows to record*
Classification Marking for this System	NHS Confidential

Further details on the classification marking scheme for NHS Information can be found in the DH NHS IG - Guidance for the Classification Marking of NHS Information 2009: https://nww.igt.hscic.gov.uk/KnowledgeBaseNew/DH_NHS%20IG%20-%20Info%20Classifications.pdf

2. System Security

2.1. Security of the system shall be governed by the CCG's Corporate Information Security Policy.

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)
<Insert Details>	*<Insert Details>*	*<Insert Details>*

Access Control: [logical security measures and privilege management]	
Registration procedures – Who will be able to access the system: *Only users who have a business need should be granted access to the system, how will this be managed, please also document whether any system training will be provided. Include detail on users who may work for other organisations*	*<Insert Details>*
Deregistration procedures – *How will users that no longer require access be managed (deactivating access) – also if users change roles and require a different level of access – please document*	*<Insert Details>*
Please list the access levels within the system:	*<Insert Details>*
Please list all privileged users of the system:	*<Insert Details>*
Recording of users and associated access levels:	*<Insert Details>*
Authentication Method: *Access control must be in place on all systems. Authentication should ideally be by username & password or two factor authentication*	*<Insert Details>*
Password Complexity:	*<Insert Details>*
Frequency of password change:	*<Insert Details>*
Number of password attempts before user account locked:	*<Insert Details>*
If system is accesses by Username and Password, can the system identify which element has been entered incorrectly:	*<Insert Details>*
Is this system accessible from Internet or only from N3?	*<Insert Details>*
Un-lock Procedures: *(Please document how a user goes about retrieving their username/password if forgotten and/or unlocking their account)*	*<Insert Details>*
In-activity time-out period:	*<Insert Details>*

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)
<Insert Details>	*<Insert Details>*	*<Insert Details>*

Additional Security Controls: *All contractors should provide assurance of their compliance with information security requirements and best practice, by means of completing the DSPT for third parties or providing an ISO27001 and cyber essentials plus 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	*<Insert Details>*
Audit Trails *(Please Specify e.g. Log on audit and whether/how this is checked/monitored)*	*<Insert Details>*
Security testing *i.e. Independent Penetration Testing Frequency*	*<Insert Details>*
Other (Please Specify)	*<Insert Details>*

3. System Management

Maintenance and 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)*	*<Insert Details>*
The System shall be implemented by:	*<Insert Details>*
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 personal data]*	*<Insert Details>*
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 (webex), N3/HSCN, VPN.*	*<Insert Details>*

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).*	*<Insert Details>*

4. System Design

Electronic Based Systems or Paper Based Systems:	*<Insert Details>*
Describe the system and purpose.	*<Insert Details>*
Describe the network that will house the system i.e. existing Bolton NHS FT, independent or cloud network?	*<Insert Details>*
Does the system require the use of a dedicated/virtual/cloud file server?	*<Insert Details>*
Does the data reside with the system software? Please state where the data resides i.e. server/ network drive / Cloud.	*<Insert Details>*
State any links to any wider network clouds e.g. site LAN, Internet and / or any other external network	*<Insert Details>*
State any firewalls / gateway control devices.	*<Insert Details>*

5. Operational Processes

Personal Data Collected:	
Will personal data be collected within the system:	*<Yes/No>* If 'no' please go to 'Storage of Data Arrangements.'
What personal data items will be collected within the system e.g. name, DOB, postcode etc	*<Insert Details>*
Will personal data be collected directly from the data subject e.g. the patient is present and providing information to the user of the system	*<Insert Details>*
Will personal data be collected from 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*	*<Insert Details>*

Will personal data be collected from paperwork: *[Please indicate security arrangements e.g. follow-up arrangements to identify lost post for posted paperwork]*	*<Insert Details>*
Will personal data be collected from CDs / Memory sticks: *[Please indicate security arrangements e.g. encryption standards]. Encryption must meet approved NHS standards i.e. 256 bit strength*	*<Insert Details>*

Storage of Data Arrangements:	
In what format (paper or electronic), where will it be stored & under what security controls?	*<Yes/No>*
Any anonymisation process for personal identifiable / special categories of data will need to be described. Please state whether this data will be shared with others and why? Will pseudonymised for all secondary purposes?	*<Insert Details>*
How (and under what security controls) will personal identifiable / special categories of data be loaded onto any file server / storage device	*<Insert Details>*
Encryption standards to be employed for stored data: *(Note - any device not in a secure area that will cache or store patient identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container. Backup copies of patient identifiable / sensitive data also need to be encrypted).* *Note - for added risk protection applicants are encouraged to encrypt patient identifiable / sensitive data stored on devices located in secure areas. Although not a NHS requirement, it may be prudent that such a step is taken should it be perceived a possibility of equipment loss or other attack*	*<Insert Details>*
How long will the data be stored for?	*<Insert Details>*

Processing of Data Arrangements:	
Paper Based Systems: *[Please describe the data handling process (referencing any flowchart at the end of the system level security procedure).*	*<Insert Details>*
Electronic Based Systems:	*<Insert Details>*

List the user devices (desktop, laptop, PDA, etc) that will access and process the data.	*<Insert Details>*
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 patient identifiable / sensitive data needs to do so on an encrypted drive, or within an encrypted container)	*<Insert Details>*
State whether remote access (over the Internet or otherwise) will be employed to access the data	*<Insert Details>*
Describe measures in place to prevent the interception of transmitted data (E.g. standalone network, encrypted path, etc)	*<Insert Details>*
Include any policy to prevent (or at the very least severely restrict) the copying of patient identifiable / sensitive data to removable media	*<Insert Details>*
If applicable, include any policy to prevent the printing of personal identifiable / special categories of data	*<Insert Details>*

Decommissioning Arrangement:	
When this system and/or its data has completed its purpose, has become redundant or is no longer needed, what methods will be followed to ensure disposal of equipment, back-up media, or ensure other stored data is appropriately undertaken	*<Insert Details>*

6. Systems Audit

6.1. The system shall be risk assessed every 12 months in accordance with the CCG's Information Risk Assessment Process.

6.2. Any improvements identified will be recorded on a security improvement plan to address all unacceptable risks.

Note:

- *Take account of cross-boundary risks / dependency issues where the system is part of a larger service or multiple CCG's arrangements*
- *A summary of this review should be provided to the Head of IT and the Cyber Security Lead and Information Governance Manager*

6.3. The system is capable of recording and auditing the following system transactions:

Audit Capability	**Yes / No, Comments**
User identification	*<Insert Details>*
Data and Time	*<Insert Details>*
Device ID used	*<Insert Details>*
Event ID/Description	*<Insert Details>*
Successful logons	*<Insert Details>*
Un-successful logons	*<Insert Details>*
Additions to the system	*<Insert Details>*
Updates made to entries (values for 'From' and 'To')	*<Insert Details>*
Deletions	*<Insert Details>*
Viewings	*<Insert Details>*
Printings – Printer ID	*<Insert Details>*
Reports Generated – including details of selection parameters	*<Insert Details>*
Extracts	*<Insert Details>*
Patient ID	*<Insert Details>*
Does the system provide easy access to extract and / or search for auditable information	*<Insert Details>*
Additional information:	

7. Systems Protection

Business Continuity Arrangements:	
Business Impact Review: *[Briefly explain/analyse the effect that a disruption might have upon the CCG's business function]*	*<Insert Details>*
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).*	*<Insert Details>*
Planning: *In the event of serious disruption or total system failure, business continuity shall be provided by the following means*	*<Insert Details>*
Confidentiality: *In the event of a security or confidentiality breach occurring the following procedure shall be provided by the following means*	*<Insert Details>* Report to Information Governance and the Information Asset Owner; Complete an incident form (via Safeguard located on the CCG's intranet) and following the Data Security & Protection Incident Reporting Policy and Procedure.

8. Data Protection Registration

Confirmation of Data Protection Registration: *Organisations are required to have a Data Protection Registration to cover the purposes of analysis and for the classes of data requested.*	
Name of Organisation	**Registration Number**
<Insert Details>	*<Insert Details>*
<Insert Details>	*<Insert Details>*
<Insert Details>	*<Insert Details>*
<Insert Details>	*<Insert Details>*

SLSP Template Ends.