NHS
Bolton Clinical Commissioning Group

System Level Security Procedure

Policy Number	**IG017**
Target Audience	**CCG/GMSS staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**December 2017**
Last Review Date	**December 2017**
Next Review Date	**December 2019**
Policy Author	**IG Manager (GMSS)**
Version Number	**V1.0**

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.

Contents

1. Introduction 4
   1.1. Systems Level Security Procedure (SLSP) Ownership 4
   1.2. Implementation 4
   1.3. Review 4
2. System 5
   2.1. System Details 5
   2.2. System Security 5
   2.3. System Management 6
   2.4. System Design 7
   2.5. Operational Processes 7
   2.6. Systems Audit 9
   2.7. Systems Protection 10

1. 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.

The following series of topics are relevant for any system level security procedure 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.

1.1. Systems Level Security Procedure (SLSP) Ownership

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.

This procedure is governed by the CCG's Information Security Policy.

This SLSP shall be available /distributed to:

Job Title	Role
<Insert Details>	

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 Privacy Impact Assessment (PIA) review carried out by the Greater Manchester Shared Services (GMSS) Information Governance (IG) Team

Completed SLSPs should be sent to the IM&T Operations Board for review and approval.

1.3. Review

An annual review of recorded SLSP's will be undertaken by the CCG's IT Department, with the assistance of GMSS 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.

2. System

2.1. System Details

Background and purpose of the system to be detailed here

Detail	Description
System known as:	*<Insert Details>*
System's Information Asset Owner:	*<Insert Details>*
System's Information Asset Administrator:	*<Insert Details>*
Data Controller:	*<Insert Details>*
System recorded on Information Asset Register:	*Yes / No (delete as appropriate)*
Flows of personal identifiable / sensitive data relevant and recorded and maintained in the Flow Mapping Tool:	*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

2.2. System Security

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

2.2.2. The System's responsible security manager is *<Insert Job Title>*

2.2.3. 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.

2.2.4. The Information Asset Owner (IAO) is accountable for:

- The secure use of the system;
- Recording and Maintaining the relevant information flows of personal confidential data (PCD) via the Flow Mapping Tool;
- Identifying and managing all Information Risks for this asset;

- Maintaining this Procedure on a regular basis at least annually.

2.2.5. The Information Asset Administrator (IAA) is responsible for maintaining the system in accordance with this procedure.

2.2.6. The system shall incorporate the following security countermeasures:

- Physical security measures (E.g. secure room, cabinet, etc)
- Logical measures for access control and privilege management
- Network security measures (E.g. firewalls, network segregation, etc)
- Other (including authentication or certification arrangements, security testing, and audit)

Note - list according to their nature i.e. technical, operational, procedural and include reference to standards used where these are known. Include areas, like keeping the system up to date (Patching/updates), dependencies

In addition – NHS organisation's are required to comply with the range of best security management practices as set out in the BS7799 / ISO 27002

Physical Security Measures

Technical	Operational	Procedural
<Insert Details>	*<Insert Details>*	*<Insert Details>*

Logical Access Control and privilege Management

Technical	Operational	Procedural
<Insert Details>	*<Insert Details>*	*<Insert Details>*

Network Security Measures

Technical	Operational	Procedural
<Insert Details>	*<Insert Details>*	*<Insert Details>*

Other (Including authentication or certification arrangements, security testing, audit)

Technical	Operational	Procedural
<Insert Details>	*<Insert Details>*	*<Insert Details>*

2.3. System Management

2.3.1. The system shall be developed / provided by:

<Insert Details>

(Note: if the system is developed or provided under commercial contract, then the relevant contract schedules that bind the contractor to the lead CCG's corporate security policy and to this system level security procedure should be referenced)

<Insert details>

2.3.2. The system shall be implemented / maintained by:

<Insert details>

If more than one, explain each specific role, include IGSOC accreditation status, if applicable

Arrangements for security configurations, repair, replacement, disposal of equipment or media that may contain patient identifiable data:

Arrangement	**Responsibility**
<Insert details>	*<Insert details>*

2.3.3. The system shall be shared or used by the following organisations:

<Insert details>

Record all participating bodies (NHS or otherwise) and their purpose

2.4. System Design

2.4.1. The system shall comprise:

To be completed in conjunction with Security Manager

If the system is paper based, please describe the elements of the systems.

For electronic based systems, describe the system and paste a simple diagram at the end of the SLSP, showing the local network that will house the system. This diagram should show the devices (e.g. file server) where the data will reside, links to any wider network clouds (e.g. site LAN, internet, and/or external networks.)

Describe the means by which unauthorised access to the system and its data will be prevented:

<Insert details>

2.5. Operational Processes

2.5.1. Personal Confidential Data (PCD) Collected

For example by on line means, paperwork through the post, data on CD. Security arrangements need to indicated, e.g. encryption standards for the on-line / CD, follow-up arrangements (to identify lost post) for posted paperwork.

<Insert details>

2.5.2. Storage of Data

i. In what format (paper or electronic), where will it be stored and under what security controls?
ii. Any anonymisation process for patient identifiable / sensitive data will need to be described.
iii. How (and under what security controls) will patient identifiable / sensitive data be loaded onto any file server / storage device
iv. 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).
iv. 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>

2.5.3. Processing of Data

For paper based systems describe the data handling process (referencing any flowchart at the end of the SLSP)
For electronic based systems:

i. List the user devices (desktop, laptop, PDA, etc) that will access and process the data.
ii. 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).
iii. State whether remote access (over the Internet or otherwise) will be employed to access the data.
iv. Describe measures in place to prevent the interception of transmitted data (E.g. standalone network, encrypted path, etc).
v. Include any policy to prevent (or at the very least severely restrict) the copying of patient identifiable / sensitive data to removable media.
vi. *If applicable, include any policy to prevent the printing of patient identifiable / sensitive data.*

<Insert Details>

2.5.4. Authorised Users

Where the system is shared across multiple legal entities it is essential to identify how this security policy will apply and how its effect will be measured

<Insert Details>

2.5.5. Decommissioning

When this system and/or its data has completed its purpose, has become redundant or is no longer needed, the CCG's Change Control Procedures will be followed to

ensure disposal of equipment, back-up media, or other stored data is appropriately undertaken.

2.6. Systems Audit

2.6.1. The system shall benefit from the following internal / external audit arrangements:

- Confidentiality Audit Procedures
- *<Insert More if relevant>*

Some systems may be subject to regular external audits, e.g. finance systems, all audit arrangements need to be listed

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

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

Take account of cross-boundary risks / dependency issues where the system is part of a larger service or multiple CCG's arrangements

2.6.3. 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>*

Add above any additional entries this system records

2.7. Systems Protection

2.7.1. The system shall benefit from the following resilience / contingency / disaster recovery arrangements:

<Insert Details>

Identify any separate plans and status

2.7.2. In the event of serious disruption or total system failure, business continuity shall be provided by the following means:

<Insert Details>

2.7.3. In the event of a security or confidentiality breach occurring the following procedure shall be provided by the following means:

- Report to Information Governance and the Information Asset Owner;
- Complete an incident form (via Safeguard located on the CCG's intranet) and following the Information Governance Incident Reporting Procedure.

All incident activity will then be in accordance with the CCG's Confidentiality Audit Procedures and Incident reporting and learning policy

2.7.4. Data Protection Registration

The CCG has a current and complete Data Protection Registration, which can be found the ICO Website; https://ico.org.uk/ESDWebPages/Entry/ZA007073

List Data Protection Registration details of other organisations involved

<Insert Details>

SLSP Template Ends.