MANCHESTER 1824

The University of Manchester

Standard Operating Procedure

Number:	UoM/System Level Security/SOP19/4.0		
Title:	**Developing and Implementing a System Level Security Policy (SLSP)**		
Version:	4.0 (August 2016)	**Effective Date**	August 2016
Author:	**Lee Moffatt**	**Review Date**	August 2018
Reviewed by : Prof Deborah Symmons		**Approved By:** Prof Nalin Thakker	
Position: Chair of Clinical Trials Management Group		**Position:** Associate Vice President for Research Integrity	
Signature:		**Signature:**	

Version	Date	Reason for change
2.0	**January 2013**	**Update of weblinks and office details**
2.1	**May 2014**	**Addition of version control statement for SOP**
3.0	**October 2015**	**Update of weblinks and office details**
4.0	**August 2016**	**Update of weblinks and office details**

When using this document please ensure that the version you are using is the most up to date either by checking on the Research Governance and Integrity Team website (http://www.staffnet.manchester.ac.uk/services/rbess/governance/) for any new versions or contacting the author to confirm the current version.

1.0 Background

In order to be compliant with the European Directive on Good Clinical Practice in Clinical Trials (2001/20/EC) organisations conducting Clinical Trials of Investigational Medicinal Products must have clearly documented Standard Operating Procedures covering all aspects of conducting Clinical Trials. The SOPs also apply to all other projects that fall under the Research Governance Framework for Health and Social Care, 2nd Edition, Department of Health 2005.

A Standard Operating Procedure (SOP) is defined by ICH Harmonised Tripartite Guideline for Good Clinical Practice as "Detailed, written instructions to achieve uniformity of the performance of a specific function". These SOPs are written instructions and records of procedures agreed and adopted by the University of Manchester.

2.0 Purpose

This Standard Operating Procedure (SOP) describes the process of developing and implementing a System Level Security Policy (SLSP).

The development, implementation and management of an 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 SLSP 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 patient identifiable / sensitive data

This SOP is underpinned by the University of Manchester's IT Security Policies (see the references section for links), based on UCISA best practice, which, in turn, draws heavily on the standards BS7799 and ISO 27001.

This SOP applies to all sensitive data relating to Trials which come under the CTIMP Regulations, where the University of Manchester is the Sponsor. The requirements of this SOP should be applied as a minimum to such trials and in conjunction with all applicable University policies and procedures and the policies and procedures of the relevant NHS Trust.

3.0 Procedure

When designing a Clinical Trial it is important to consider how trial-related data will be collected, stored and processed for the duration of the trial. This is likely to include the design of any computerised systems that will be required to assist with the management of trial data. Paramount in the design will be the security of the data management system and the data itself.

The IT Security Checklist (see SOP Computerised Systems for Clinical Trials: Appendix 1) should be completed initially and returned to Lee.Moffat@manchester.ac.uk for review, to ensure that some fundamental aspects of data management and IT Security are being considered. Examples of areas which should be addressed are:

- data processing
- data transmission
- computer and data security
- physical security
- data archiving
- IT and information security awareness, procedures and training

IT Security will review the completed checklist and dependant on responses, will arrangea site visit if required to audit existing IT systems and working processes and provide guidance around best practice in data handling, IT and information security best practices. IT Services staffwill also work with trial staff to implement and support trial related computer systems. Visit arrangements can be made via the University's IT Service Desk (see the contact list section for details).

A template for the production of an SLSP can be found in Appendix A.

4.0 Related Procedures and references

SOP Data Management

SOP IT Security and Encryption

SOP Computerised Systems for Clinical Trials – Site Set Up and Initiation

UoM Cyber Security website:

http://www.itservices.manchester.ac.uk/cybersecurity/
UoM Data Protection website
http://www.dataprotection.manchester.ac.uk/

Contact list

The University's IT Service Desk
t: 0161 306 5544

w: http://www.itservices.manchester.ac.uk/help/

Research Governance and Integrity Team
http://www.staffnet.manchester.ac.uk/services/rbess/governance/

Appendix A: Template for the production of a System Level Security Policy

System Details	
The system is known as:	
The system's responsible owner is:	
The system's Caldicott Guardian or Data Controller is:	
System Security	
Security of the system shall be governed by the corporate security policy of:	
The system's responsible security manager is:	
The security manager's responsibilities shall include:	
The System will incorporate the following security countermeasures:	
• Physical Security – Data Processing:	
• Physical Security – Data Hosting:	
• Access Control and Privilege Management:	
• Network Security Measures:	
• Other:	
System Management	
The system shall be developed / provided by:	
The system shall be implemented and maintained by:	
The system shall be shared or used by the following organisations:	
System Design	
The System shall comprise:	
Operational Processes	
The patient identifiable / sensitive data will be collected:	
The data will be stored:	
The data will be processed:	
The system's authorised users shall be:	
When the system or its data has completed its purpose, has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:	
System Audit	
The system shall benefit from the following	

internal / external audit arrangements:	
The system shall be risk assessed (frequency):	
System Protection	
The system shall benefit from the following resilience / contingency / disaster recovery arrangements:	
In the event of serious disruption or total system failure, business continuity shall be provided by the following means:	
In the event of a security or confidentiality breach occurring the following procedure shall be followed:	
SLSP Ownership	
This SLSP shall be the responsibility of:	
This SLSP shall be available / distributed to:	