eMBED Health Consortium

System Level Security Policy Toolkit

|  |  |
| --- | --- |
| **Version** | 0.1 |
| **Version Date** | June 2016 |
| **Date Due for Review** | July 2017 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Amendment** |
| 0.1 | C Wallace | June 2016 | First draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Introduction 4](#_Toc453745198)

[Document Compilation Guidance 4](#_Toc453745199)

[Guidance on Completion of SLSP 4](#_Toc453745200)

[1 Document Control 4](#_Toc453745201)

[1.1 Scope 4](#_Toc453745202)

[1.2 Audience 4](#_Toc453745203)

[1.3 Distribution List 4](#_Toc453745204)

[1.4 Amendment Details 4](#_Toc453745205)

[1.5 Review 4](#_Toc453745206)

[2. System Details 5](#_Toc453745207)

[2.1 Configuration System Documentation Registers 5](#_Toc453745208)

[2.2 Equipment 5](#_Toc453745209)

[2.3 Software 5](#_Toc453745210)

[2.4 Additional Features Of System 5](#_Toc453745211)

[2.5 Interfaces with Other systems 5](#_Toc453745212)

[2.6 System Roles 5](#_Toc453745213)

[2.7 Support Services 5](#_Toc453745214)

[2.8 Data Protection 5](#_Toc453745215)

[2.9 Requests for Information 6](#_Toc453745216)

[2.10 Procedure in the event of a suspected security breach 6](#_Toc453745217)

[3. System Security 6](#_Toc453745218)

[3.1 Physical Security 6](#_Toc453745219)

[3.2 Workstations 7](#_Toc453745220)

[3.3 Network 7](#_Toc453745221)

[4. Authorised Users 7](#_Toc453745222)

[4.1 Users Management 7](#_Toc453745223)

[4.2 Access Control (Passwords & Identities) 7](#_Toc453745224)

[4.3 Training & User issues 7](#_Toc453745225)

[5. Fault & Change Management 8](#_Toc453745226)

[5.1 Fault Management & Business Continuity 8](#_Toc453745227)

[5.2 Disaster Recovery Procedures 8](#_Toc453745228)

[5.3 Change Control 8](#_Toc453745229)

[5.4 Support & Third Party Access 8](#_Toc453745230)

[5.5 Log 8](#_Toc453745231)

[6. Housekeeping Procedures & System Integrity 8](#_Toc453745232)

[6.1 Back Up Regime 8](#_Toc453745233)

[6.2 Back up storage 9](#_Toc453745234)

[6.3 Restoring from Back Ups 9](#_Toc453745235)

[6.4 Protection from virus & malicious software 9](#_Toc453745236)

[7. Other Housekeeping and Security Procedures 9](#_Toc453745237)

[7.1 Checking for failed Log On’s 9](#_Toc453745238)

[7.2 Risk Assessment 9](#_Toc453745239)

[7.3 Procedures Documentation 9](#_Toc453745240)

[Templates 10](#_Toc453745241)

# Introduction

All systems in use within the organisation requires a System Level Security Policy (SLSP) as detailed in the Information Security Policy. The aim of the SLSP is to ensure that the organisation considers how these systems will be managed on a day to day basis to ensure that operation remains secure from the provision of user access to data connections between systems. If controls in place at a higher level fail then systems are required to have own security controls in place and ensure that if the system is damaged data can be recovered within an acceptable business timeframe.

SLSP’s developed are departmental documents which do not require approval for use. Once completed a copy should be forwarded to the IG Team to allow the document to be used as evidence for the organisations IG Toolkit submission.

# Document Compilation Guidance

The following series of headings and descriptions should be consider for all system level security policies 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 department/system 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.

Also provided as part of this toolkit is a completed example of an SLSP and a template SLSP containing suggested wording which can be amended to reflect operation of the system.

# Guidance on Completion of SLSP

The following headings and number reflect those contained within the template SLSP.

## 1 Document Control

###  Scope

This section sets out which systems are covered by the content of this document and gives a brief description of what the system is used for.

### Audience

In this section please detail who is expected to read and follow the details within the SLSP.

### Distribution List

Detail where this document will be available for staff within the department to access it

### Amendment Details

Allows the development and amendment to the document to be recorded and requires the application of version numbers to avoid confusions in identification of the latest version of the SLSP.

### Review

Sets the date for the SLSP to be reviewed. This should be annually to ensure minor changes to working practices are reflected.

## System Details

### Configuration System Documentation Registers

In this section please list, or attach, documentation regarding the use or configuration of the system such as a supplier operating manual.

### Equipment

In this section details on the physical equipment used to run the system is added. This would be servers to run a database but would also include any specific hardware e.g. bespoke scanner.

### Software

This table is used to record what software is used to run the system or which is installed on the server. This should include details of the operating system on the server.

### Additional Features Of System

### Interfaces with Other systems

This section is used to detail if the system has any interfaces which allow for the import or export of information from the system. This could be automated system to system transfers or manual transfers were data files are received and imported into the system.

### System Roles

Details of who is the Information Asset Owner for the system along with details of the Information Asset Administrator should be added here to clarify overall responsibility for the system at a department/directorate level.

### Support Services

This section details the support arrangements in place for the system. In almost all cases details of the local IT provider should be added for first line support e.g. computer doesn’t have network connection. Details should also be provided of any support arrangements with the system supplier and a description of what support is available.

### Data Protection

Where systems hold and/or process personal confidential data (PCD), data that identifies an individual, this section should be completed.

#### Data Protection Officer

Identifies who in the organisation is responsible for data protection.

#### Caldicott

Identifies who the organisations caldicott guardian is.

#### Data Protection Registration

Confirms and provides the organisations data protection registration details as submitted to the Information Commissioners Office. These can be looked up directly by visiting <https://ico.org.uk/esdwebpages/search>. If you find that upon review the registration does not cover the type of data been processed please contact your organisations IG Lead who may need to amend the registration.

#### Data Classification Statement

This section clarifies how the data within the system is classified in regards to the organisations Records Management or Information Security Policy.

#### Data Controller

Who is the data controller? Please add in details regarding data controllership and what their relationship is e.g. data controller in common or joint data controllers

#### Legal Justification for Holding Data

All PCD that is processed by organisations requires a clear legal basis to conduct the processing. This is a legal requirement. Without a clear legal basis an organisation may be in breach of the law and subject to heavy financial penalties.

Legal justification can include requirements under a separate piece of legislation for the collection and processing of this information. In this case the legal act and subsection requiring the processing should be referenced.

Legal basis could also be through the collection of explicit consent of the individuals. Explicit consent needs to be recorded so please describe how this is obtain and where it is stored.

#### Validation of Data

This section should be used to detail how information collected is validated. This could be done through the patient demographic service which allows names and addresses as well as registered GP Practice to be confirmed. Another example of this is that when a patient checks in the receptionist checks their details to the system.

#### Printout and/or Reports

Are print outs or reports generated from the system which contain PCD? If so then processes around how these are managed to ensure information remains secure even after it leaves the system.

#### Data Disposal

Enter details of how the information will be managed/disposed of following the end of the contract with the supplier. Will they hand back the information in a usable format or will they hold it until disposal. What assurance will be provided that the data will be safe and securely disposed of?

#### Data Security

If the data is held by a third party provider will it be encrypted to offer an additional level of security?

### Requests for Information

How will requests for information be dealt with in regards to the system? Detail how subject access requests and freedom of information requests will be managed if different from the organisation wide policy.

### Procedure in the event of a suspected security breach

What is the process in place for reporting of security breaches? Detail how such a breach would be managed referencing the organisation wide policy on incident reporting.

## System Security

This section provides details on how security is managed and associated responsibilities.

### Physical Security

This section is used to describe where the servers used to run the system are located and what physical and environmental controls are in place to protect them. Where servers are hosted by a third party details should be obtain from the supplier regarding their management.

### Workstations

Some systems have dedicated applications installed on the user’s computer to allow them to access it. This section can be used to detail how access to the system from a user device is achieved and how installation of any client application will be controlled. With the adoption of web enable applications which use a web browser, e.g. Chrome, to access the system client applications may not be required.

Where the system holds and processes personal confidential data additional restrictions on an end user may be required such as having privacy filters fitted to screen to stop inadvertent disclosure of information to passing staff in an open office.

### Network

This section should be used to detail if there are any network restrictions in regards to the system. This could be limiting the computers able to connect to the server e.g. only approved IP or hostname can access the server. This section can also be used to detail how the system is secured across the internet, if it is at all.

## Authorised Users

This section details with user controls and required training.

### Users Management

Use this section to detail the controls in place for managing new users, amendment to job roles and leavers. Please detail if this system is based on a role based access profiles and provide definitions of what access is possible within each profile and how requests for each type are approved.

Details should include references to any request forms used within the process. Staff leavers and the lack of notification to system owners has always been a management challenge. Ensure that within the leaver’s process that there are details of how dormant accounts will be identified and removed along with the frequency that this is will performed and how formal evidence of its completion is maintained for audit purposes.

Please note that review of accounts with elevated privileges should be performed more frequently than user reviews. User’s reviews should be completed at least annually.

### Access Control (Passwords & Identities)

Details on password settings e.g. changed every 90 days should be included here. Consideration should be given to forcing password changes for a user upon first logon, password expiry period, min and max password lengths and if passwords have to meet any complexity requirements.

This section can also be used to record session time out, this is when an idle user is automatically logged out or if the system has any time restrictions on access e.g. 9am-5pm Monday to Friday.

### Training & User issues

Please details any pre-requisite training that is required to be completed before access to the system will be granted. Also any other training available with regard to the system should be detailed along with the frequency it should be undertaken.

This section can also be used to detail any other user restrictions in place not previously documented.

## Fault & Change Management

### Fault Management & Business Continuity

In this section you should provide details of how faults are reported, monitored and resolved. The IAO or IAA should maintain a log of faults reported and expected resolution times. This allows the management of third party providers to KPI’s set in their contracts.

Please also provide details of the departments business continuity plan. Details should confirm that a plan is in place and the system discussed in this document is included as well as providing information on where and who holds a copy.

### Disaster Recovery Procedures

This section deals with the technical recovery of the system following an incident. You should agree a recovery point objective (RPO) (how frequently the system will be backed up and therefore the maximum amount of data that will be lost following an incident) and the recovery time objective (RTO) (how quickly does the system need to be functioning again) with the IT department or system supplier.

It is not necessary to include step by step details on how the system is recovered from backup tapes or reinstalled but it should be confirmed with IT that such a process is in place and reference it. Such as process could be added as an appendix. Details should be included on how often the DR Plan will be tested, responsibilities for this testing and how evidence will be retained of the testing and any lessons learnt.

### Change Control

Computer systems can be updated by manufacturers to fix or add functionality. Changes can also come about due to process changes within the department that require reflecting in how the system is setup to process data. This section should be used to detail how change requests are made, approved and any forms involved in the process. There may be two process here one for changes to settings within the system and another for changes to the platform enacted by the IT department. When making changes to critical systems these are normally made to a replica system so that they can be tested prior to their implementation on live systems.

### Support & Third Party Access

Please provide details of how support companies can, if at all, access the system either on site or remotely. This should include how access is achieved technically, who authorises it and limitations on such access e.g. Supplier can access the system upon request to and approval of the IAO. Access will be provided to the server via an RDP session which will only remain enabled until 5:00pm the same day.

### Log

This section should be used to detail what logging/audit records are maintain within the system. If the system holds and/or processes personal confidential data then it is a requirement that logs are maintained of who has accessed which records and when.

## Housekeeping Procedures & System Integrity

This section is used to document technical arrangement for the systems backup. Where the system is a fully hosted service by a third party it should be confirmed that arrangements are in place to meet the agreed RTO and RPO. Specific details in the sections below are not necessary for fully hosted third party systems.

### Back Up Regime

This section details who is responsible for the backing up of the system, what method is used to perform the backup and how often.

### Back up storage

Please provide details of where backups are stored and for how long they will be retained. Please ensure that you consider records retention guidelines when setting these.

### Restoring from Back Ups

Detail how restores are performed, approved and any planned restores.

### Protection from virus & malicious software

This section can be used to detail how the system is protected from malicious software such as viruses.

## Other Housekeeping and Security Procedures

Please provide details of any regular activities that are performed in the management of the system but which have not been detailed previously

### Checking for failed Log On’s

This could include the IAA checking for failed logon attempts. A surge in failed logon attempts may indicate that the system is under attack.

### Risk Log

A risk log for the system should be produced and this section details responsibilities for completing this risk log, how it is maintained and where it is stored. The completed risk log should be embed within the SLSP document or hold together with it. Once complete both documents should be sent to the IS Team for review. Any residual risks will be noted and if above the risk acceptance threshold should be added to the department risk register and if necessary the corporate risk register. Template for a risk log is located in the templates section.

### Procedures Documentation

This section should be used to reference any working policies, standard operating procedures or any other documentation related to the management of the system not already identified elsewhere in the SLSP.

# Templates

Example completed SLSP TBC

Template SLSP 

Risk Log Template 