mul(

In Support of the Data Security and Protection Toolkit

System Level Security Policy

Any new questions have been highlighted in YELLOW and must be c

NOTE Q5.13 to 5.10 have been added in red to support the migration to MS Office 365 - if these may not function correctly.

Asse

System Name:

Hospital Site:

Division:

Directorate:

Directorate Manager:

Excluded from Review: ☐ Exclusions can only be authorised by the DSP team once assurance regarding data retention is provided.

Reason for exclusion:
IE Retired / Not in service

Submission Date:

Review Date:

Completed by:
(AD login or email)

Review and completion of the following sections is required annually, or more frequently changes to the system.

1 Introduction.

The SLSP is a core component of an accreditation documentation set for those organisations that undertake fo information assets. NHS organisations are required as part of the Data Security and Protection requirements to information systems.

This document template is generated in line with the latest Data Security and Protection requirements, and the te
at any point to incorporate new requirements.

Completed SLSPs must be reviewed at least once every 12 months.

2 Responsibilities.

Data Security and Protection Exec Group

The objective of Data Security and Protection is to protect the personal information of patients and staff whilst pr
to Trust corporate information. A Data Security and Protection
structure provides individuals and partner organisations with evidence based assurance that personal and corp
securely, and efficiently in order to assist in the delivery of the best possible ca

The Data Security and Protection Exec Group (DSPEG) supported by the Data Security and Protection Manag
effective policies and management arrangements to identify risk and associated aspects of IG in accordar

IGSG members provide specialised IG knowledge and/or guidance, to ensure that all IG requirements are ap
specific projects. The IGSG membership includes divisional representation

To ensure that the Trust adheres to the fundamental aims of IG and the requirements of the contained the Da

Caldicott Guardian

All NHS organisations must appoint a Caldicott Guardian which is a role that is an amalgamation of managemen
the involvement of healthcare professionals in relation to achieving improved Data Security and Protection con
responsibility for ensuring that all staff conforms to the Caldicott Principles and the guidance contained in the N
The Caldicott Guardian (CG) will guide the Trust on confidentiality and protection issues relating to patient inforr
balance between maintaining confidentiality standards and the delivery of patient care. The CG will also advise t
issues as they arise.

Senior Information Officer (SIRO)

It is a mandatory requirement for the Trust nominate a Senior Information Risk Officer (SIRO). This should be a
be responsible for the ownership of information risk across the Trust and to undertake the role of SIRO. The SIR
the Trust's strategic business goals may be impacted by information risks and the links with risk management ar
is strategically responsible for Information Security and Information Risk across th

Data Protection Officer (DPO).

Informing and advising UHNM on Data Protection regulations, and national law or Data Protection provisio
policy with Data Protection regulations, national law or Data Protection prov

IT Clinical Risk Lead

In line with ISB standard DSCN18 the Trust is required to have an IT Clinical Risk Lead, who must report to
This role ensures that relevant risk management processes are followed to minimise any risks to patient sa
use of software products. The IT Clinical Risk Lead must be independent rather than part of

Information Asset Owner

Information Asset Owners are routinely responsible for locally managed information system are directly accoun
assurance that information risk is being managed effectively in respect of the information assets that they are
Owners are senior individuals involved in running the relevant business. Their role is to understand and addres
'own' and to provide assurance to the SIRO on the security and use of those as
IAO are responsible for completing and maintaining relevant asset documentation for Information Assets they ma

Information Asset Administrator

Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident r
IAA's generally manage the day to day aspects of maintaining an Information Asset, i.e. running backups, ensur

3. System Details

Information assets are identifiable and definable assets owned or contracted by organisations which are valuable to the business of that organisation. It is vital that al and each assigned to an Information Asset Owner (IAO)

IAO's are directly accountable to the SIRO and will provide assurances that information risk is being managed effectively for their assigned information assets.

3.1 System IAO:
(Responsible Owner):

3.2 System IAA:
(Responsible administrator) OR ☐ UHNM ICT Operations Team

3.3 Description of the System:

3.4 Approx. number of System users:

3.5 Approx. number of data subjects in the system ie patients / staff:

3.6 Is this a replacement for a previous system YES ○ NO ○

If yes please provide details:

3.7 Is there an approved DPIA in place:

3.8 Is there a DTAC in place for the system

3.9 Primary (Live) Location of System:

3.10 Secondary / Backup Location of System:

3.11 Does this system connect to a medical device? YES ○ NO ◉

3.11.1 If yes, please name the device

3.12 Is this system business critical to the Trust? YES ○ NO ◉

3.13 Is this system business critical to your department? YES ○ NO ◉

3.14 Existence of automated decision-making, including profiling: YES ○ NO ◉

3.15 Please select the relevant asset classification(s) for the system:

- ☐ P1A - A system that is critical for patient care: (i.e. emergency care, diagnostic)
- ☐ P1B - A system that is critical for patient care: (i.e. emergency admission, monitoring, 7/7 service)
- ☐ P1C - A system that is critical for patient care: (i.e. outpatient, elective admission, core business hours)
- ☐ P2 - A system that is used for patient registration, communication and affects the Hospital financially or reputationally
- ☐ P3 - A system that adds efficiencies

3.16 Is this system patient facing? i.e. will it be used by patients YES ○ NO ◉

3.16.1 If patient facing does the system integrate with the NHS app

3.17 Is the system used to provide remote patient monitoring:

3.18 Patient Pathway Function:

3.19 Do you have completed DCB0160 documentation in place for this system

3.19.1 If N/A please confirm why

3.19.2 DCB0160 Documentation Review Date

4. Data Protection, Caldicott Guardian & Data Flows Considerations

It is important that each IAO should be aware of what information is held, and the nature or justification for information flows to and from the information asset for whi

It is a legal responsibility of an organisation to ensure that data transfers of personal information for which they are responsible are secure at all stages. Any such dat

The loss of personal information will result in adverse incident reports which will adversely affect the organisations reputation but if this is carried out intentionally or r

UHNM Caldicott Guardian
IT Clinical Risk Lead
Chief Clinical Information Officer: Zia Din
Deputy Clinical Director - Medicine
Zia.din@uhnm.nhs.uk
01782 554244

UHNM SIRO: Amy Freeman
Director of IM&T
Amy.Freeman@uhnm.nhs.uk
01782 672472

Data Protection Officer (DPO): Leah Carlisle
Head of Data, Security & Protection
DPO.UHNM@uhnm.nhs.uk
01782 676493

4.1 Does this system hold Patient or Staff Identifiable Information? YES ◉ NO ○

- ☐ Appointment
- ☐ Clinical
- ☐ Demographic
- ☐ Mobile Phone Number
- ☐ Results
- ☐ Other - Please provide details below

If YES please provide details:

4.1 b Does this system contain data relating to under 18's YES ○ NO ○

If other ie financial or corporate please provide details:

4.2 Is this system NHS Number Compliant? YES ○ NO ○ NA ☐ (ie no patient information)

If this system is not fully NHS Number Compliant you will be required to complete an additional audit with details of any areas of non compliance.

4.3 Is the data held in the system encrypted at rest? YES ○ NO ○

4.4 Does this system meet all current GDPR and data protection requirements? YES ○ NO ○

4.5 Has National Data Opt-out been applied to the patient data within the system?

4.6 Please briefly describe all information flow into this system;

4.7 Please briefly describe all information flows out of this system;

4.8 Is the system capable of anonymising or pseudonymising data sent from or extracted from the system?

- ☐ Full details only
- ☐ Anonymised
- ☐ Pseudonimised

4.9 Is any Patient or Staff Identifiable Information from this system routinely sent to OR received from outside the UK?

YES ○ NO ○

If yes please specify where: EEU ☐ US ☐ Other (Please specify):

4.10 Safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable):

- ☐ Adequacy Dec
- ☐ Contract
- ☐ DPA
- ☐ IDTAs

4.11 Does this system interface to another Trust system? ☐

If yes please identify the system (s)

4.12 Is this system integrated with the Trust's EPR (Careflow/iPortal)?

4.13 Is this system integrated with the Trust's PACs System:

4.14 Does this system use HL7 messaging? ☐

4.14 Data Flows Mandatory Requirements: *All information flows to and from a system, both within the Trust and external need to be captured and risk assessed on a Data Flow As generated manually. All data flows for your system must be included in the form which can be accessed here .*

4.15 Common Law duty of confidentiality:

4.16 Article 6 lawful basis for processing personal data:

4.17 Article 9 condition for processing special category data:

4.18 Legitimate interests for the processing (if applicable):

4.19 The source of the personal data (if applicable):

4.20 Categories of recipients:

- ☐ UHNM Staff
- ☐ Other NHS Orgar
- ☐ Patient
- ☐ External Process/

4.21 Does the asset involve a joint controller?

4.22 Name and contact details of joint controller (if applicable):

4.23 How long is the data stored in this system retained for?

5. Software and Software Supplier

Supplier

5.1 Who is the supplier for the system software?

5.2 Supplier contact details:

5.3 Is there an SLA or OLA or contract in place for this system? YES ○ NO ○

5.3.1 When does this expire?

5.4 Where are the documents stored?

5.6 Is this managed under the Trusts PFI agreement? YES ○ NO ◉

5.7 Contract / SLA Reference

5.8 Contract Renewal Date

5.9 Does the Supplier hold ISO27001 certification

5.10 Does the Supplier hold Cyber Essentials certification

5.11 Supplier registered with ICO YES ○ NO ◉ **ICO Registration Number**

Software

5.10 What system software is installed for this system?

5.11 What version of this software is currently installed?

5.12 What is the latest version of the software ?

5.13.1 Does this involve the use of apps?

Yes ○
No ◉

5.13.2 If apps are used

On Trust owned staff devices ☐
On personally owned staff devices ☐
On patient owned devices ☐

5.12 Please list any supporting software for this system

5.13 Has the supplier provided their DCB0129 documentation for the system?

5.13.1 If N/A please confirm reason:

5.14 Please can you confirm after how long does the system session timeout?

OFFICE 365 MIGRATION

This section has been added for 2021 to support the Trusts move to the NHS O365, if these details are unavailable if may impact system functionality.

5.13 Does this system interface with Microsoft Office Applications at all?

5.14 Which office packages does it interface with - please select all that apply

- ☐ Word
- ☐ Excel
- ☐ Power point
- ☐ Access
- ☐ Publisher

5.15 Please describe how it interfaces with Office

5.16 Is this system compatible with O365

5.17 Does this require a local (desktop) install of 365 or can it use the web version

5.18 Is a system upgrade needed to provide this compatibility

if yes please provide details below

5.18 a If an upgrade is needed what it the indicative cost

5.18 b If a system upgrade is needed will this require infrastructure changes?

5.19 Please add any additional associated details or comments

5.20 O365 Responses Complete yes / no (project team)

5.21 What Operating System does the server use?

5.22 Does this system use any shared components ie shared SQL databases etc? YES ☐

5.23 Does this system have the Trust standard Anti-Virus and Anti-Malware protection installed?

YES ○ NO ○

If no please provide details of what is in place.

Software / Application support details

5.24 What arrangements are in place for software failure?

5.25 Support contact details if different to supplier details:

5.26 Is there a separate support / maintenance agreement other then the contract in section 5.7 YES ○ NO ◉

If yes please provide details:

5.27 Does the system received regular operational and security patches or updates from the supplier? YES ○ NO ◉

5.28 Does any third party have access to the system, i.e. remote access to server to provide support? YES ○ NO ◉

5.29 If yes is their access 24/7 or restricted hours access? 24/7 ○ Restricted ◉

5.20 Contracted Support Hours
ie Mon- Fri 8-5

6. Hardware

6.1 Is this hosted within the Trust, or externally

For **Externally hosted** systems:

6.2 If externally is this physical or cloud storage

Details of external hosting requirements including name of hosting company and data centre:

6.3 What Cloud model is used for this system:

Platform as a Service PaaS ☐
Infrastructure as a Service IaaS ☐
Software as a Service SaaS ☐

For **Internally hosted** systems:

6.3 What server hardware is this system installed on?

6.4 Server name

6.5 What type of server is this?

☐ Physical
☐ Virtual
☐ Clustered
☑

If other please provide details

6.6 Who is the supplier for this hardware

6.7 What desktop hardware is used to access this system?

6.8 Maintenance arrangements,
callout times and fix times if appropriate

6.9 Is the server under Warranty? YES ○ NO ◉

If yes when does the Warranty Expire?

6.10 Contact details for 3rd party

6.11 Do any incidents with this server follow the Trusts normal call logging and escalation procedure?

YES ○ NO ○

6.12If no please provide details of call logging procedures

7. Risk Assessment

It is an Data Security and Protection Requirement that all Information Assets have a risk assessment carried out and the results be recorded.

Please refer to RM01 for details as to how to carry this out. A template is available to use.

Risk assessments require review at least yearly, more often if there are significant changes to the system.

ALL HIGH RISKS IDENTIFIED SHOULD BE INCLUDED ON THE TRUST RISK REGISTER (DATIX) IN LINE WITH TRUST POLICY.

8. Physical / Logical Security

Protection of equipment is necessary to reduce the risk of unauthorised access to data and to protect against loss, damage, theft or compromise of information asset

Threats to a system should be identified as part of that systems risk assessment.

Precautions are also required to prevent and detect the introduction of malicious and unauthorised mobile. Failure to protect against viruses and other malware could care.

Please add details any measure not listed below.

- ☐ *Trust Standard Anti-Virus
- ☐ *Trust Standard Malware Protection
- ☐ *UPS
- ☐ *Surge Protection
- ☐ *Trust Standard Firewall
- ☐ *Restricted Access Area
- ☐ *Air Conditioning
- ☐ *Food and Drink Free Area
- ☐ RAID
- ☐ Mirrored Server
- ☐ Clustered Server
- ☐ Fire Protection
- ☐ Multiple server room locations
- ☑

9. Access Controls

Access to information systems, information processing facilities and business processes should be controlled on the basis of business need and security policy requi where these exist, for information dissemination and authorisations

Group ID's prevent successfully audits being carried out that trace actions to an individual and should therefore only be used if absolutely necessary and in locally ap users with access to this ID.

9.1 What is the approval process for gaining access to the system?

9.2 Who authorises access to the system?

9.3 Who allocates user profiles and access levels?

9.4 How are access levels allocated?

9.5 What different levels of access are available?

9.6 What records are kept of authorised users?

9.7 Are unnecessary accounts removed? YES ○ NO ◉

9.8 What is the process for removing users (leavers or movers from the system?

9.9 Do you receive a monthly copy of the staff leavers list? Yes ○ No ◉

9.10 Do you remove access based on the staff leavers list? Yes ○ No ◉

9.11 Who is responsible for removing users from the system?

9.12 Please identify any other access control methods used for this system?

IE Restricted login hours, multi factor authentication

10. Password Control

All computer systems should have at logon authentication process that includes at least a unique user ID and password, some systems may require additional contro

10.1 Does this system allow individual usernames and passwords? ◉ YES ○ NO

10.1.1 Is the system integrated with the Trust's Active Directory?

10.2 How are risks regarding confidentiality and security mitigated if the system does not support individual logins?

10.3 Does the system support the use of Multi-Factor Authentication (MFA) ? YES ○ NO ○

10.3.1 If Yes is it supported through integration with the Trust's Active Directory only: YES ○ NO ○

10.3.2 If Yes please confirm how MFA is used:
- ☐ **Remote Support from provider**
- ☐ **Trust privileged accounts**

10.3.3 If MFA is used what authenticator tool or device is used:

10.3.4 If MFA is not used please choose the appropriate exemption:

10.4 Are group logins permitted for the system? YES ◉ NO ○

If yes please provide details;

10.5 Does this system have usernames and passwords in addition to users AD login and password? YES ◉ NO ○

All AD user passwords follow the rules below;

PASSWORD
Minimum Length = 12 characters
Maximum password age = 90 days
Minimum password age = 2 days
Enforced password history = 12 password remembered
ACCOUNT LOCK OUT
Lock out activated = 3 failed attempts

AD Controls

Which AD Security Group does the user need to be added to for application access?

Which AD Security Group does the user need to be added to for Power User access?

Which AD Security Group does the user need to be added to for Administrator access?

Non AD Controls

A) What is the minimum password length?

B) Required password format
- ☐ Must Contain Letters
- ☐ Must Contain Numbers
- ☐ Must contain non alpha-numeric
- ☐ Must Contain Captials
- ☑

C) Does the system support the use of a passphrase? YES ◉ NO ○

D) Must the password be changed on first use? YES ◉ NO ○

E) Can users change their own passwords? YES ◉ NO ○

F) How long it the password valid for?

G) Can passwords be reused? YES ◉ NO ○

H) Will repeated invalid attempts cause the account to lock out? YES ◉ NO ○

I) How many attempts will lock the account?

J) How long with the lock out last?

10.6 Method of notifying initial password?
- ☐ Letter
- ☐ E-mail
- ☐ Via Manager
- ☐ On Training Course
- ☐ Verbal

11. Audit Trail

Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedur

All systems should be routinely audited to ensure:
- *The current list of users is correct*
- *Users have the right access levels*
- *Users are only accessing data in accordance with their job role and associated policies*
- *Data quality*

11.1 Please list any Audit trails / logs available for this system. (i.e failed logins, viewed/ amended records)

11.2 Where are these audit records stored?

11.3 How long are these records retained for?

11.4 Who has access to these records?

11.5 Have any audits been run in the past 12 months? YES ○ NO ◉

Please provide details

12 . Staff Training

12.1 Is training compulsory before being given access to the system? YES ○ NO ○

12.2 Who is responsible for booking staff on relevant training courses?

12.3 Who carries out the training courses?

12.4 What type of training is used?

☐ Classroom
☐ One to One
☐ On line
☑

Please add any other methods used

12.5 What records are kept of users trained?

12.6 Who has access to the training records?

13. Data Backup

Networked data that is stored on servers should normally be backed up on a daily basis as a minimum by the system administrator or by automated processes. Back from which it was created.

13.1 How often is a backup run for this system?

13.2 What media is this backed up to?

13.3 Are backups Manual? ○ Automated? ○

13.4 Where is the backup media stored?

13.5 What information is backed up?

13.6 Who is responsible for running the backups?

13.7 Who has access to the backed up data?

13.8 How long is backup data kept for?

13.9 How often is a test restore carried out?

14. Security Incident Management and Reporting

All Trust staff have a responsibility to report any real or potential breached of information security i.e. unauthorised access, non-availability of the system etc.

All operational issues with the system should be reported in the first instance to the ICT service desk, unless other incident reporting systems have been agreed and

ALL INFORMATION SECURITY EVENTS / INCIDENTS OR NEAR MISSES MUST BE REPORTED ON DATIX FOLLOWING THE TRUSTS INCIDENT REPORTIN

14.1 Are there any active DATIX incidents for this system? YES ○ NO ◉

14.2 Does this system use the Trusts ICT reporting channels for faults / incidents? YES ○ NO ○

14.3 This system is supported by clinical technology ☐

If no please provide details of reporting arrangements

14.4 Is the IAO for this system fully aware of the reporting path for operational and security issues with this system? YES ○ NO ○

15. Business Continuity and Disaster Recovery

Documented procedures and information (a business continuity plan) should be maintained for all information assets, these will be used in the case of an incident to

Risks to the confidentiality, integrity and availability of information assets must be regularly assessed. This plan should be regularly reviewed and tested through simu

15.1 Is there a documented Business Continuity plan for this system? YES ○ NO ◉

15.2 Who is responsible for Business Continuity Planning?

15.3 Is there a disaster recovery plan in place for this system? YES ○ NO ◉

15.4 Who is responsible for Disaster Recovery Planning?

15.5 Is there any spare / hot-swap hardware available in case of hardware failure? YES ○ NO ○

15.6 Is there an alternative location which could be used to restore services? YES ○ NO ○

15.7 If appropriate what are the timescales for replacement hardware to be provided and where would this be sources from?

15.8 Who is responsible for restoring this service?

15.9 Are there any single points of failure within this system which could impact continuity?

15.10 Have you every had to restore / recover this system? YES ○ NO ◉

15.11 Have you every been unable to restore / recover data in this system? YES ○ NO ◉

16. Change Control

All organisations experience change in one form or another. Rapidly changing technology has a major impact on processes and systems already in place, often requ personal information. It is vitally important that the impact of any proposed changes to the organisations processes and / or information assets are assessed to ensur

16.1 Is this system currently covered by formal change control? YES ○ NO ○

16.2 Who is required to authorise any changes?

17. Future of Project

17.1 Are there currently any planned changes for this system? YES ○ NO ○

If yes please provide details;

17.2 Is there a current retirement date for this system? YES ○ NO ○

18. Supporting Documentation

Please upload any supporting documentation relating to this information asset, this can include, but is not limited to SOPs, guides, SLA or contract information etc.

Click here to attach a file

Review Status

Completion status (2018/2019)

Completion Status (2019/2020)

Completion Status (2020/2021)

Completion Status 2021/2022

I agree that this review is now complete for 2022/23/24

DSP Comment

Submit