great people great place

NHS Isle of Wight NHS Trust

SYSTEM LEVEL SECURITY POLICY

Policy Type	Non Clinical
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Information Security Manager
Next Author Review Date	1st May 2022
Approving Body	Policy Management Sub-Committee 9th October 2018
Version No.	4.0
Policy Valid from date	1st October 2018
Policy Valid to date:	31st October 2022

'During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Advisory Group and where necessary other relevant Oversight Groups'

This document forms part of the suite of documents for Isle of Wight NHS Trust's ISO|IEC27001:2013 Information Security Management System (ISMS). As such, it is continuously monitored via the Information Governance Sub-Committee (IGSC).

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved Versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
25-02-16	1	25/02/2016	Executive Director of Strategy & Planning, ICT and Estates.		Approved at Trust Executive Committee
8-12-16	1.2		Executive Director of Strategy & Planning, ICT and Estates.	Review	Information Governance Steering Group
13-12-16	2.0	13/12/2016	Executive Director of Strategy & Planning, ICT and Estates.	For approval	Corporate Governance and Risk Sub-committee
30/10/17	2.1		Director of Strategy & Planning	Annual Review	
09/11/17	2.1		Director of Strategy & Planning	For Ratification	Information Governance Steering Group
12/12/17	3.0	12/12/2017	Director of Strategy & Planning	Approved at	Corporate Governance and Risk Sub-Committee
13/09/18	3.1		Executive Director of Finance, ICT and Estates.	Endorsed at	Information Governance Sub-Committee
09/10/18	4.0	09/10/2018	Executive Director of Finance, ICT and Estates.	Approved at	Policy Management Sub-Committee
29/01/21	4.0	09/10/2018	Director of Finance, Estates and IM&T	12 month blanket policy extension due to covid 19 applied with author review date set 180 days prior to Valid to Date.	Quality & Performance Committee
22/05/21	4.0	069/10/2018	Director of Finance, Estates and IM&T	Extended policy uploaded and linked back with new cover sheet	Corporate Governance

NB This policy relates to the Isle of Wight NHS Trust hereafter referred to as the Trust

Contents

1. Executive Summary

The development, implementation and management of a system level security management policy, supported by an Information Asset Register which captures relevant information for each information asset used by the Trust will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of the Trust.

In order to have in place effective system level security arrangements, Information Asset Owners will be required to ensure that they review the Information Asset Register in relation to each information asset that they have responsibility for at least annually. This register will 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. The information asset register will also be used to identify information risks, which will be registered on the risk register at the commensurate level in line with the Trust Risk Management Strategy and Policy

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of person identifiable / protectively marked data.

2. Introduction

As a Trust it is imperative that we take steps to ensure the security of all information assets that we utilise to prevent data or information being available inappropriately. The Trust is required to comply with a range of specific security measures some of which are set out within this policy.

Current encryption guidance for NHS organisations can be obtained from ICT or from NHS Digital. It would be expected that any electronic solution for the handling of person identifiable/sensitive data to comply with this guidance as a minimum.

In addition - 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 management policy is a core component of an accreditation documentation set for organisations that undertake formal accreditation processes for their information assets.

Where the system is available to multiple organisations, the system level security management 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.

The following series of topics are relevant for any system level security policy and are intended to help guide responsible staff through their considerations for the development of their system level security measures. 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.

The requirement for the completion of the Information Asset Register will be captured at either

- The procurement stage of new or replacement systems, or,
- The Privacy Impact Assessment (PIA) review, which will be considered and where appropriate authorised by the Information Governance Sub-Committee.

3. Definitions

3.2 Information Asset

The National Archives defines an Information Asset as “a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively”.

Therefore in essence an Information Asset is ‘any record’ that is created, whether that be electronic on a bespoke database, or on a spreadsheet or in paper form.

Information Assets can hold information about the following:-

- Patients (clinical record, electronic or paper, includes emails, letters, scans etc.)
- Staff (HR record, supervision and appraisal, sickness and leave, training, disciplinary, capability etc.)
- Business Information (Financial, performance, quality, governance, SAR, FOI etc.).

Therefore our information assets are all the systems we employ to capture the above.

3.3 Information Asset Owner

IAOs are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’. IAOs may be assigned ownership of several assets within their organisation. The register of IAOs is held and maintained by the Information Governance department, and is available to staff on request.

3.4 Senior Information Risk Owner

The Trust SIRO must be an Executive Director or member of the Senior Manager. The SIRO has overall responsibility for the Trust’s Information Governance Policy including the Management of Information Risks, and also leads and implements the IG risk assessment and advises the Board on the effectiveness of information risk management across the Trust.

The SIRO will act as champion for information risk on the Board and provide written advice on the content of the Trust’s Statement of Internal Control in regard to information risk.

The SIRO must understand the strategic business goals of the Trust and how other organisation’s business goals may be impacted by information risks, and how those risks may be managed.

4. Scope

This Policy must be followed by all Information Asset Owners in discharging their duties. However, the Policy also sets out specific responsibilities for the Senior Information Risk Owner, and the Information Governance Lead Officer.

5. Purpose

The purpose of this policy is to set out what is required from Information Asset Owners in relation to the completion of the information asset register annually.

6. Roles and Responsibilities

6.2 Information Asset Owner (IAO)

Information Asset Owners are responsible for identifying all information assets used across their areas of responsibility and ensuring clarity with regards to who owns the information asset. They must update and review the Information Asset Register as a minimum annually, or where there is a change of asset use or ownership, although quarterly reviews are recommended.

6.3 Information Security Manager / Information Governance Lead Officer

The Information Security Manager, alongside the Information Governance Lead Officer, must ensure that they review the Information Asset Register Quarterly and ensure that matters for escalation, such as significant information risks are dealt with or escalated expediently. They will produce a 6 months report for the Information Governance Steering Group, in relation to the Information Asset Register and any associated risks.

6.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is accountable for ensuring that the Trust has in place a robust information governance framework. A fundamental part of this framework is ensuring that systems employed are secure, and meet IG requirements.

The SIRO is the Accountable officer for information security for the Trust.

7. Policy Detail/Course of Action

All Information Asset Owners must review and revise the information asset register on an annual basis as a minimum, or where changes have occurred to ensure that the register remains up to date and all associated information risks have been identified and are being mitigated where possible. The Information Governance Sub-Committee (IGSC) will review the register and a report produced by the Information Governance Lead Officer on a 6 monthly basis.

All staff members that are likely to introduce new information processes or information assets are required to obtain approval from the IGSG at the proposal stage of the new process or asset

The register must be updated where possible prior to an information asset being brought into operation. Prior to the introduction of a new system, a Privacy Impact Assessment must also be undertaken and approved by the Information Governance Sub-Committee. Where information risks are identified these must be reported in line with the Trusts Risk Management Strategy and Policy, and escalated as appropriate.

8. Consultation

The following groups have been consulted in the preparation of this document:-

1. Information Governance Sub-Committee
2. ICT Group
3. Information Asset Owner Forum

The Information Governance Sub Committee was consulted on the changes for this version

9. Training

There is no specific training requirement associated with this policy; however, support will be

available, from colleagues in ICT, Information Governance, and the Information Security Manager.

10. Monitoring Compliance and Effectiveness

The Information Asset Register will be reviewed annually during an Information Asset Owners forum to ascertain that all information assets are being managed effectively by the IAO's. A report on the findings of this review will be presented at the Information Governance Steering Group.

11. Links to other Organisational Documents

- Risk Management Strategy and Policy

12. Appendices

- A Financial and Resourcing Impact Assessment on Policy Implementation
- B Equality Impact Assessment (EIA) Screening Tool

Appendix A

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	**System Level Security Policy (no change in commitment from previous iteration)**

Totals	**WTE**	**Recurring £**	**Non Recurring £**
Manpower Costs			
Training Staff			
Equipment & Provision of resources			

Summary of Impact:

Risk Management Issues:

Benefits / Savings to the organisation: Equality Impact Assessment

- Has this been appropriately carried out? YES/NO
- Are there any reported equality issues? YES/NO

If "YES" please specify:

Use additional sheets if necessary

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	**WTE**	**Recurring £**	**Non-Recurring £**
Operational running costs			
Totals:			

Staff Training Impact	**Recurring £**	**Non-Recurring £**
Totals:		

Equipment and Provision of Resources	Recurring £ *	Non-Recurring £ *
Accommodation / facilities needed		
Building alterations (extensions/new)		
IT Hardware / software / licences		
Medical equipment		
Stationery / publicity		
Travel costs		
Utilities e.g. telephones		
Process change		
Rolling replacement of equipment		
Equipment maintenance		
Marketing – booklets/posters/handouts, etc.		
Totals:		

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	
Signature & date of financial accountant:	
Funding / costs have been agreed and are in place:	
Signature of appropriate Executive or Associate Director:	

Appendix B

Equality Impact Assessment (EIA) Screening Tool

Document Title:	System Level Security Policy
Purpose of document	Set out the Trust arrangement for system level security
Target Audience	*Information Asset Owners, and Administrator, and other staff with specific responsibilities relating to Information Governance*
Person or Committee undertaken the Equality Impact Assessment	*Carl Moreira-Smith*

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?

- If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.
- If yes please detail underneath in relevant section and provide priority rating and determine if full EIA is required.

		Positive Impact	**Negative Impact**	**Reasons**
Gender	Men	*N/A*	*N/A*	
	Women	*N/A*	*N/A*	
Race	Asian or Asian British People	*N/A*	*N/A*	
	Black or Black British People	*N/A*	*N/A*	
	Chinese people	*N/A*	*N/A*	
	People of Mixed Race	*N/A*	*N/A*	
	White people (including Irish people)	*N/A*	*N/A*	

	People with Physical Disabilities, Learning Disabilities or Mental Health Issues	*N/A*	*N/A*	
Sexual Orientation	Transgender	*N/A*	*N/A*	
	Lesbian, Gay men and bisexual	*N/A*	*N/A*	
Age	Children	*N/A*	*N/A*	
	Older People (60+)	*N/A*	*N/A*	
	Younger People (17 to 25 yrs.)	*N/A*	*N/A*	
Faith Group		*N/A*	*N/A*	
Pregnancy & Maternity		*N/A*	*N/A*	
Equal Opportunities and/or improved relations		*N/A*	*N/A*	

Notes:

Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3. Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	**NO**
Legal (it is not discriminatory under anti-discriminatory law)			
Intended			

If the negative impact is possibly discriminatory and not intended and/or of high impact then please complete a thorough assessment after completing the rest of this form.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:

3.2 Could you improve the strategy, function or policy positive impact? Explain how below:	
3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?	
Scheduled for Full Impact Assessment	Date:
Name of persons/group completing the full assessment.	
Date Initial Screening completed	11-11-16