Network Security Policy

Version:	3.2
Approved by:	Senior Leadership Group (SLG)
Date Approved:	21/06/2022
Document reference:	NHIS.042
Document Type:	Policy
Responsible Strategic Business Unit:	Technical Operations
Document Manager:	Head of Technical Operations
Lead Director:	Chief Technical Officer
Date issued:	28/06/2022
Review date:	21/06/2024
Target Audience:	All NHIS staff and organisations accessing resources through the NHIS Network.
NHIS Policy Template Version Control	**Version 4.2 May 2022**

Contents

Document Control

Document location

Location
NHIS Intranet Hub - NHIS Policies And Procedures - All Documents (sharepoint.com)

Revision history

Version	Issue Date	Job Title of Person/ Name of Group circulated to	Brief Summary of Changes
2.4	August 2017		Reviewed in line with NHS Digital Guidance
2.5	September 2017		Reviewed and updated following review by Information Governance, Management and Technology Committee
2.6	September 2017		Job titles amended and referenced to NHS Digital template policies.
2.7	October 2017		Approved at Health Informatics Strategy Board pending minor revisions.
3.0	November 2017		Reviewed and agreed by Head of Technical Solutions
3.0.1	November 2019	Corporate Assurance Manager	Transferred to current NHIS standard policy document template. Added sections: 2.4, 6 & 25 & appendix 1. Updated job titles and ISO ref from ISO:2013 to 2017. Assigned corporate policy number.
3.0.2	06/12/2019	Network & Communications Manager	Minor amends
3.0.3	December 2019	Head of Governance & Assurance	Added Quick Reference Guide
3.1.1	29/04/2022	Corporate Assurance Manager	Transferred to new Policy template. Minor updates applied (hyperlinks, job titles, document titles updated).
3.1.2	03/05/2022	Head of Technical Operations	None
3.1.3	03/05/2022	Senior Third Line Engineer (Networks & Comms)	None
3.1.4	20/05/2022	Network & Comms Manager	None
3.1.5	14/06/2022	Senior Leadership Group	None

Approvals

Version	Approval Date	Approval Group
2.7	October 2017	Health Informatics Strategy Board (pending minor revisions).
3.0	November 2017	Reviewed and agreed by Head of Technical Solutions
3.1	January 2020	Approved by SLG
3.2	21st June 2022	Senior Leadership Group (SLG)

All NHIS policies can be provided in audio, large print, Braille or other formats and languages on request.

This is an official document. Whilst this document may be printed, the electronic version posted on the intranet is the official copy.

Quick Reference Guide

For quick reference, the guide below is a summary of actions required to ensure appropriate implementation of this policy. This does not negate the need for the document manager and others involved in the process to be aware of and follow the detail of this policy.

1. This document sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network and establishes the responsibilities for network security.

2. Access to the network shall be obtained by use of a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network shall conform to the Electronic Remote Working Policy and to partner/customer local policy and NHS best practice.

3. All users to the network shall have their own individual user identification and password and are responsible for ensuring that their password is kept secret and never shared.

4. User access rights shall be immediately removed for those users who have left the organisation and reviewed for those users who have changed job role. This is actioned by NHIS upon the organisation informing the NHIS Service Desk of those changes.

5. Third party access controls shall be in place and confidentiality and security status ascertained for third parties prior to accessing the network. All third-party access to the network shall be audited.

1. Introduction

1.1. This document defines the Network Security Policy for Nottinghamshire Health Informatics Service (NHIS). The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network. This document sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network and establishes the responsibilities for network security.

1.2. The network is a collection of communications equipment such as servers, computers, smart devices, printers and switches that have been connected either by cables or associated wireless equipment. The network is created to share data, software, and peripherals such as printers, Internet connections, hard drives and other data storage equipment.

2. Purpose

2.1. Inadequate configuration and management of networks will lead to vulnerabilities that could be exploited by internal or external attackers. The exploitation of such vulnerabilities may incur damage to the Nottinghamshire Health Informatics Service business function and that provided to our client organisations, through the loss, compromise or corruption of information or data and/or the loss of system facilities or system access.

2.2. NHIS has a requirement that any network employed to support the business function, shall be available when needed and can be accessed only by legitimate users.

2.3. The aim of this policy is to assure the security of Nottinghamshire Health Informatics Service's (NHIS) network. To do this NHIS will:

a) Ensure Availability of the network
b) Ensure that the network is available for authorised users only.
c) Preserve Integrity of the network
d) Protect the network from unauthorised or accidental modification
e) Preserve Confidentiality of the network
f) Protect associated assets against unauthorised disclosure.

2.4. The Nottinghamshire Health Informatics Service network shall be available when needed subject to the agreed Service Level Agreements /Key Performance Indicators with partner and customer organisations. The network can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity, and confidentiality.

2.5. Nottinghamshire Health Informatics Service shall comply with other laws and legislation as appropriate.

2.6. Network Operating Procedures are in place to set out the correct and secure operation of the network and are developed and maintained by NHIS. These have been developed in line with the ISO 27001: 2017 standard of information security management.

2.7. This policy is aligned to the ISO 27001:2017 standard controls for 'A.13.1 – Network security management' and in line with information security policies and procedures.

Control Ref	Title
13.1	Network security management
13.1.1	Network controls
13.1.2	Security of network services
13.1.3	Segregation in networks
9.1.2	Access to networks and network services
12.2.1	Controls against malware

3. Scope

3.1. This policy applies to all networks supported by Nottinghamshire Health Informatics Service used for the storage, sharing and transmission of clinical and non-clinical data and images; for the printing or scanning of clinical or non-clinical images or data and for the provision of internet systems for receiving, sending and storing both clinical and non-clinical data and images.

3.2. Nottinghamshire Health Informatics Service (NHIS) is hosted by Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) and as such all employees of NHIS should abide by the corporate policies of the host organisation (such as those relating to HR and Information Governance), although NHIS will own any technical IT policies that apply to the network and ICT Infrastructure.

3.3. NHIS provides ICT services across a number of partner and customer organisations, some of which are non-NHS and these individual organisations shall have their own corporate policies relating to Information Security, Acceptable Use and Confidentiality.

The Network Security Policy references local organisational policies or their equivalents as below:

Information Security Policy
Electronic Remote Working Policy
Confidentiality and Data Protection Policy
Safe Haven Procedures
Internet and Email Policy
Secure Disposal of IT Equipment and Media Policy (NHIS)
Anti-Malware Policy (NHIS)
Mobile Devices Policy

The list is not exhaustive, and the relevant policies will be maintained by the relevant partner organisations in line with national and NHS requirements.

3.4. The policy follows the principles set out in the ISO 27001:2017 standard for Information Security (ref: section 2.4) and complies with standards set out in the Data Security & Protection Toolkit (DSPT).

3.5. Where a network connects to the Health and Social Care Network (HSCN) it is essential that the information security management standards applied to the local network are sufficient to prevent untoward threats arising to the HSCN or the information assets of its other affected connections.

4. Definitions

shall	This term is used to state a Mandatory requirement of this policy
should	This term is used to state a Recommended requirement of this policy
SyOps	Security Operating Systems
CRAM	NHIS Compliance, Risk and Assurance Management (CRAM) Group
SLG	Senior Leadership Group within NHIS
SBU	NHIS Strategic Business Unit

5. Roles and Responsibilities

5.1. NHIS shall ensure that roles and responsibilities for management of the network, desktop devices and associated software and hardware is allocated appropriately within the service and that adequate resources are available to provide the service.

The Head of Technical Operations is responsible for ensuring that NHIS complies with the below statements:

5.2. Nottinghamshire Health Informatics Service **shall**:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy framework in a consistent, timely and cost-effective manner.
- Ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensure the security of the network, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations and in accordance with NHIS business needs, policy and guidance.
- Ensure the development and application of network security Standards and Procedures, in accordance with the NHIS network, is limited to those who have the necessary authority and clearance.
- Ensure there is a central point of contact on network infrastructure security for both staff and external organisations.
- Lead in the formulation of network security Standards and Procedures.

- Co-ordinate network security activities, particularly those related to shared information systems or IT infrastructures.
- Approve tested systems and agree plans for implementation.
- Support security incident investigations and assessments where necessary.

5.3. Partner and Customer Organisations / Managers **shall**:

- Ensure that staff are aware of their security responsibilities.
- Ensure that staff have had suitable security training.
- Ensure that the NHIS Service Desk is promptly notified when new accounts are required.
- Ensure that the NHIS Service Desk is promptly notified when existing accounts are to be reviewed or deleted, for example, when a member of staff changes roles or leaves the organisation.

5.4. Users **shall**:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems and follow organisational security policy.
- Ensure their password is kept secret - passwords should not be shared under any circumstances.
- Report on any suspected or actual breaches in security.

5.5. Senior Information Risk Owners (SIRO) **shall**:

- Meet the applicable legal requirements and ensure that operational compliance is further delegated to the Information Asset Owners (IAO).

6. Equality and Diversity Statement

6.1. This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1.

6.2. This document is not subject to an Environmental Impact Assessment.

7. Risk Assessment

7.1. Nottinghamshire Health Informatics Service shall carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments shall cover all aspects of the network that are used to support those business processes. The risk assessments identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

7.2. These shall be conducted on a regular basis and remedial actions and countermeasures shall be put in place in relation to identified risks within an agreed timescale. Risk assessments shall be conducted using appropriate industry recognised standard methodologies.

8. Physical & Environmental Security

8.1. Critical or sensitive network computer equipment **shall** be housed in an environment that is monitored for temperature, humidity and power supply quality.

8.2. Critical or sensitive network equipment **shall** be housed in secure areas, protected by a secure perimeter, with appropriate security barriers, security camera and entry controls. Physical controls such as intruder alarms and fire suppression systems shall be in place.

8.3. Critical or sensitive network equipment **shall** be protected from power supply failures.

8.4. Door codes shall be changed periodically, immediately following a compromise of the code.

8.5. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

8.6. All visitors to dedicated secure network areas must be authorised *prior to any visit* and shall be made aware of network security requirements which includes the requirement to log in and out of the secure areas, as per the Access to Server Room Procedure.

8.7. Entry to secure areas housing critical or sensitive network equipment shall be restricted to those whose job role requires it and the authorised list shall be reviewed regularly.

9. Access Control to the Network

9.1. Access to the network shall be obtained by use of a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network shall conform to the Electronic Remote Working Policy and to partner/customer local policy.

9.2. There shall be a formal, documented user registration and de-registration procedure for access to the network. Organisational departmental managers or heads of service must approve user access prior to access being actioned by the NHIS Service Desk.

9.3. Access rights to the network shall be allocated on a strict ‘Need to Know’ (NTK) basis and will allocated on the requirements of the user's job role, rather than on a status basis. Access will be granted under least privilege principles.

9.4. Security privileges (i.e., 'super user' or network administrator rights) to the network shall be allocated on the requirements of the user's job role, rather than on a status basis and these elevated rights shall be reviewed by the employing organisation.

9.5. All users to the network shall have their own individual user identification and password and are responsible for ensuring that their password is kept secret and never shared.

9.6. User access rights shall be immediately removed for those users who have left the organisation and reviewed for those users who have changed job role. This is actioned by NHIS upon the organisation informing the NHIS Service Desk of those changes.

9.7. Third party access controls shall be in place and confidentiality and security status ascertained for third parties prior to accessing the network. All third-party access to the network shall be audited.

10. Wireless Networks

10.1. Users **shall** connect to wireless networks via authorised and managed access points.

10.2. Network access will be prioritised for clinical services.

10.3. Wireless networks **shall** utilise the latest approved level of encryption and the latest approved authentication protocol.

10.4. Unauthorised devices connected to the wireless network **shall** be blocked with no warning.

10.5. Staff **shall** only connect personally owned wireless devices to the public or staff wireless networks. No corporate access will be given to personal devices.

11. External Network Connections

11.1. All connections from external networks and systems shall conform to the NHS-wide Network Security Policy, Code of Compliance and supporting Department of Health guidance.

11.2. All connections from external networks and systems shall be reviewed, documented and approved by NHIS before they commence operation

12. Connection of Non NHIS Supplied Devices to the Network

12.1. Connection of non-NHIS devices to the network should be approved by the requesting organisation on the understanding that the devices must comply with agreed security protocols.

12.2. Configuration specific to NHIS supported organisations has provided a MINIMUM criterion for the safe connection of devices ensuring that the configuration complies with organisational requirements and relevant UK Law. This MINIMUM criterion has been shared with all NHIS customers receiving network services.

13. Maintenance Contracts

13.1. The Head of Technical Operations shall ensure that maintenance contracts are maintained and periodically reviewed for all network equipment where such support is deemed to be required. All contract details constitute part of Nottinghamshire Health Informatics Service's Information Asset register.

13.2. All third-party organisations that have access to the network must complete a security assessment as it is NHIS's responsibility to ensure that the integrity of the network is maintained, and that contracts and operating procedures are in place.

13.3. Formal agreements for the exchange of data and software between organisations shall be established and approved by the relevant data controller and the equivalent NHIS officer as a data processor.

14. Data Backup and Restoration

14.1. Backups shall be taken regularly in accordance with the Backup Procedure and specific system requirements.

14.2. A log **shall** be maintained of switch configuration and data backups detailing the date of backup and whether the backup was successful.

14.3. Documented procedures for NHIS managed backup processes and storage of backup tapes (if used) shall be implemented and communicated to all relevant staff. All backup tapes (if used) shall be stored securely, and a copy will be stored off-site, in line with any media usage policies/procedures.

14.4. Documented procedures for the safe and secure disposal of NHIS managed backup media shall be implemented and communicated to all relevant staff (ref: Secure Disposal of IT Equipment and Media Policy).

14.5. The restoration from a backup **shall** be tested regularly and the process documented; the restoration testing **should** be at least annually.

15. User Responsibilities, Awareness & Training

15.1. NHIS shall ensure that all their users of the network are provided with the necessary security guidance, awareness and where appropriate training on information security and confidentiality.

15.2. All users of the network must be made aware of the contents and implications of the Network Security Policy and their local organisational information security and confidentiality policies.

15.3. Irresponsible or improper actions by any users may result in disciplinary action(s).

15.4. All users must ensure that they protect the network from unauthorised access. They must log off the network when finished working and lock their screens if away from their workstation, in accordance with organisational clear screen procedures.

16. Accreditation of Network Systems

16.1. The network shall meet the appropriate operating approvals and configuration management system and shall not pose a security risk to the organisations supported by NHIS.

16.2. A log of all faults on the network shall be maintained and reviewed according to an agreed procedure including any countermeasures applied, *this **should** be quarterly*.

16.3. NHIS will ensure that the network conforms to the latest cyber and data security policy and good practice guidance from NHS Digital's Data Security Centre and advisory notices are reviewed and acted upon (CareCERT Programme).

17. Malicious Software

17.1. Measures shall be in place to protect the network from malware, viruses and other malicious software. The network shall be monitored to ensure protection from internet or email based cyber security threats in line with UK Government guidance.

18. Unauthorised Software

18.1. Use of any non-standard software **shall** be approved by the organisation and NHIS management before installation.

18.2. All software **shall** have a valid licence agreement.

19. Secure Disposal or Re-Use of Equipment

19.1. NHIS shall ensure that hardware and IT equipment for disposal will be undertaken securely as set out in the Secure Disposal of IT Equipment & Media Policy

19.2. It is the responsibility of NHIS Customer and Partner organisations to ensure that equipment for disposal is retained securely until collected by NHIS for destruction.

20. System Change Control

20.1. NHIS **shall** ensure that appropriate change management processes are in place to review changes to the network, which would include acceptance testing and authorisation.

20.2. The Head of Technical Operations may require checks, or an assessment, of the actual implementation based on any proposed changes prior to any change to systems being implemented, in accordance with NHIS Change Management and Control processes.

20.3. Network Security Policies, design documentation, security operating procedures and network operating procedures shall be updated and reviewed regularly and in line with NHS operating guidelines.

20.4. All hardware or software shall meet agreed security standards.

20.5. Testing facilities shall be used for all new network systems. Development and operational facilities shall be separated.

21. Security Monitoring

21.1. NHIS **shall** ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

21.2. NHIS **shall** retain the right to disconnect or block any device connected either by physical or wireless means to the network where a security risk is identified or suspected.

21.3. NHIS **shall** retain the right to block any physical non-approved device connected to a piece of NHIS owned equipment.

22. Reporting Security Incidents & Weaknesses

22.1. All potential security breaches shall be investigated and reported through the NHIS Incident Reporting and Management Procedure and then to the **Compliance Risk and Assurance Management Group (CRAM)** if escalation is required.

22.2. Security incidents and weaknesses identified by customer or partner organisations must be reported to the NHIS IT Service Desk and reported in accordance with the requirements of the organisation's incident reporting procedure.

22.3. Security incidents or breaches shall be reported to customer organisations according to their specific Service Level Agreements and agreed Key Performance Indicators.

23. Business Continuity & Disaster Recovery Plans

23.1. NHIS s**hall** ensure that business continuity and disaster recovery plans are produced for the network and that these are tested on a regular basis.

23.2. The plans are reviewed by the NHIS Senior Management team and tested on an annual basis or where there are significant changes to the network infrastructure.

24. References

24.1. Internal References:

- Information Security Policy
- Electronic Remote Working Policy
- Confidentiality and Data Protection Policy
- Safe Haven Procedures
- Internet and Email Policy
- Secure Disposal of IT Equipment and Media Policy (NHIS)
- Anti-Malware Policy (NHIS)
- Incident Management and Reporting Procedure (NHIS)

24.2. External References:

- ISO\IEC 27001:2017 – Information technology – Security techniques - Information Security Management Systems - requirements

24.3. Nottinghamshire Health Informatics Service shall comply with:

Copyright, Designs & Patents Act 1988
Access to Health Records Act 1990
Computer Misuse Act 1990
The Data Protection Act 1998
The Human Rights Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2012

25. Monitoring Compliance and Effectiveness

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring** **e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)**
Compliance with policy	Security & Risk Officer	Internal Audits	As per internal audit schedule	Senior Leadership Group (SLG) Compliance, Risk & Assurance Management Group (CRAM)
Compliance with policy	Chief Technical Officer	Network penetration testing by authorised third party.	Annually	NHIS Director Senior Leadership Group (SLG) Summary report presented to Partnership Board
IT Health Checks	Chief Technical Officer	IT security testing by authorised third party.	Annually	NHIS Director Senior Leadership Group (SLG) Summary report presented to Partnership Board

26. Training Requirements

26.1. There are no mandatory training requirements for NHIS staff associated with this policy.

27. Review and Revision

27.1. The policy shall be presented to the NHIS Senior Leadership Board (SLG) for ratification.

27.2. This policy shall be reviewed every 2 years or where there are significant changes to the network infrastructure or operating procedures.

28. Appendices

28.1. Appendix 1 - Appendix 1 - Equality Impact Assessment Form (EQIA)

APPENDIX 1 - Equality Impact Assessment Form (EQIA)

Name of service/policy/procedure being reviewed: Network Security Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 29/04/2022			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	Availability of this policy in languages other than English	Alternative versions can be created on request	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this document	Already in font size 11. Use of technology by end user. Alternative versions can be created on request	None
Sexuality	None	Not applicable	None

Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

None for this version, in that all previous principles remain in accordance with previous version (which was subject to consultation) and this version is primarily a reformat and codification of agreed practices.

What data or information did you use in support of this EqIA?

Trust policy approach to availability of alternative versions

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

NO

Level of impact

From the information provided above and following EQIA guidance document Guidance on how to complete an EIA
Low Level of Impact

Name of Responsible Person undertaking this assessment: Sandra Greasley

Signature: *S. Greasley*

Date: 29/04/2022