ACCOUNT MANAGEMENT AND ACCESS POLICY

POLICY

Reference	IG/012		
Approving Body	Data Protection and Cyber Security Committee		
Date Approved	17th November 2025		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	January 2026		
Version	4		
Summary of Changes from Previous Version	Changes to this policy include sections on zero trust principles, third parties and incident reporting.		
Supersedes	3		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Data Protection and Cyber Security Committee		
Date of Completion of Equality Impact Assessment	23rd July 2024.		
Date of Environmental Impact Assessment (if applicable)	23rd July 2024.		
Legal and/or Accreditation Implications	UK General Data Protection Regulation Data Protection Act 2018 Network and Information Systems Regulation		
Target Audience	All staff		
Review Date	2 years		
Sponsor (Position)	Data Protection and Cyber Security Committee		
Author (Position & Name)	Director of Corporate Affairs, SIRO (Senior Information Risk Owner)		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security & Privacy		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
1. Information Security Policy	July 2025
Template control	April 2024

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Line Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures, and user obligations applicable to their area of work.
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security.
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using.
- Ensuring staff know how to access advice on information security matters.

1.1. Inactive user accounts may appear harmless, but can cause significant impact on the organisation operationally, especially where they are not disabled or remain on the system without expiry limits. Outside intruders trying to hack into an organisation can use these accounts and the activities potentially remain undetected. Staff members who leave the organisation or transfer departmentally can misuse their login credentials to access network resources.

1.2. The damage caused to the network depends on the intruder's skill and the level of privileges they possess If a user can still log into servers, access confidential data, or even just access the organisations resources, they can wreak havoc that can cause reputational damage and breach UK Data Protection Act 2018.

1.3. Access to systems should be based on the principle of 'least privileges'. Least privilege means giving a user account only those privileges which are essential to perform its intended function; this applies to everyday users and to system and application administrators. Its aim is to enhance the protection of data and information processed and the IT/software functionality from faults and malicious behaviour.

These procedures in this policy apply especially to new starters, change of job role, long-term absence, and leavers. This policy also includes all contractors, agency and third party staff.

2.0 POLICY STATEMENT

2.1. This document has been developed to maintain a secure network for SFH and its partners.

The Trust is committing to the principles of the policy and protection of the shared network through management of user accounts. The Trust will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official business.

2.2. The policy describes how access controls are applied by the organisation, covering all stages in the life cycle of user access, from the initial registration process to the final de-registration of users who no longer require access to the organisations information systems and services.

2.3. As a rule, IT systems should be secured as much as possible without inhibiting business requirements.

If hardware and software (operating systems and programmes/applications) are not securely configured the number of potential vulnerabilities is increased and this makes the systems more at risk of not only being attacked but exploited with data breaches, loss of service and reputational damage as the result. Every organisation should aim to either have, or contractually require, its IT systems to be configured as securely as possible.

2.4. This policy is aligned to the ISO 27001:2022 standard controls for management and monitoring of access controls.

Control Ref	Title
A.5.15	Access control
A.5.16	Identity management
A.5.17	Authentication information
A.5.18	Access rights
A.8.2	Privileged access rights
A.8.5	Secure authentication
A.8.18	Use of privileged utility programs

2.5. This policy applies to all staff, including those on temporary contracts, contractors, placements, and staff on secondment. It also applies to third parties doing work on behalf of the organisation and with access to the organisational assets and data.

2.6. The policy covers all devices owned or connected to the IT network at any site owned or leased by the organisation/customer site or from a remote location from where NHS staff may connect to this network.

2.7. Permission may also be granted for users to remotely access clinical information systems from non-NHS sites/private homes using Remote Desktop Access (Virtual Private Network or Desktop on Demand). The same security principles will apply.

3.0 DEFINITIONS/ ABBREVIATIONS

Active Directory (AD) Accounts	User account management system. Accounts refers to all network access, Health and Social Care Network (HSCN) access, individual system access and access to information systems through smartcards

IT Equipment	Any device provided by NHIS including any directly connected storage devices and removable media
Network	A group of two or more computer systems linked together
Corporate Network	The local and wide area network controlled by NHIS for the use of NHIS and its supported organisations
NHIS Customer Portal	https://customerportal.notts-his.nhs.uk/
Information Asset Administrator (IAA)	The person responsible for the upkeep, configuration, and reliable operation of information systems, including paper-based systems
Information Asset Owner (IAO)	Information Asset Owners are senior individuals who can be held accountable should an information security incident occur within their Division / department. The IAO's role is to: • Understand and address risks to the information they 'own' • Provide assurance to the SIRO (Senior Information Risk Owner) on the security and use of the information they own.

4.0 ROLES AND RESPONSIBILITIES

The Cyber Security Assurance Programme (CSA) has developed these documents to further ensure the security of the shared network and infrastructure. They have been developed by the CSA Delivery Group, consulted on by each partner by their internal governance and then approved by the CSA Programme Board**.**

4.1. It is the responsibility of each staff member to adhere fully to the requirements of this policy. Directors or designate heads of department and line managers are responsible for implementing this policy within their respective areas.

4.2. The line manager of the relevant staff member is responsible for performing tasks associated with initial registration, user changes, and the final removal of the user. The NHIS Service Desk will action requests to process account amendments upon the appropriate instruction from the organisation.

4.3. It is the responsibility of the system administrator (Information Asset Administrator) to ensure that housekeeping tasks are undertaken on the system on a regular basis (such as review of current users and access rights).

4.4. All individuals who access, use, or manage systems provided by NHIS are responsible for reporting any breach of this policy to the appropriate manager via the Datix incident reporting system or via the information governance team, line manager and the NHIS Service Desk.

5.0 APPROVAL

Approval of the Policy will be through the Cyber Security Assurance Programme Board, with appropriate consultation through relevant Trust officers and the Information Governance Working Group. The Data Protection and Cyber Security Committee will formally accept the Policy for the Trust and ensure that Trust Staff are aware of the principles of the Policy.

6.0 DOCUMENT REQUIREMENTS

6.1. Principles

Identification and authentication shall be used to identify and prove which users have accessed and utilised the organisation's systems and the data within them.

The degree of authentication (single or 2 factor) shall be assessed for the level of protection required for the processed information and the risk factors to it by the Information Asset Owner (IAO) and Senior Information Risk Owner (SIRO). Where it is deemed 2 factor authentication is required, the authentication mechanisms shall be provided by different methods – e.g. password and token.
Passwords shall be used to ensure that access to NHS systems, devices and information is controlled and restricted to approved and authorised users only. Passwords shall be complex in nature and follow HMG guidance and best practice.

Systems should be configured to force the change of passwords at regular intervals. These intervals should be of sufficient frequency to aid security, but not too frequent that this causes problems for users and administrators.

6.2. Granting User Access

Access to SFH and NHIS managed information systems is controlled through a formal user registration process as detailed in organisational induction and an onboarding process supported by the Information Governance and Security Policies in place at that organisation.

Each user, including third parties accessing SFH and NHIS hosted systems, is identified by a unique user ID so that users can be linked to and held accountable for their actions.

Access to managed and supported systems provided by the NHIS Service can be requested via Service Desk through the customer portal and can only be permitted after proper procedures are completed by the employing organisation. Partner organisations are responsible for requesting an account through the NHIS Customer Portal.

For system/network accounts, a new user will be set up on receipt of the instruction to the NHIS Service desk. Login details and passwords will only be provided to the owner of the

account (or line manager if this is set up prior to commencement in post if this has been agreed through NHIS).

On first logon to a new user account, the user must change the default password assigned to the account. Logon details must not be shared with others and an individual's account must not be used as a generic account.

Any access request to a network shared drive area that is not given by default will only be granted following approval from the line manager or a designated staff member. Access requests to restricted folders must be authorised by the folder owner or a designated staff member along with details of the access permissions required.

Generic or shared accounts will not be set up unless there is a valid business reason and the organisation has the appropriate governance in place. These accounts must have a valid business user associated with them. Generic accounts (accounts that are not attributed to a single user) do not facilitate an audit trail, in that there is no way to determine who was using the account at any time unless a separate log is kept. It is also difficult to attribute actions to an individual (for example, accessing an inappropriate website).

Requests to systems that are not supported by NHIS must be requested from the relevant IAO of that system and account management procedures documented in the relevant standard operating procedure for that business area.
Remote access may be granted to fulfil an organisation's business needs as described in its information security policies. The requirements for user registration and de-registration remain the same as standard network users.

6.3. Modifying/ Movers User Access

Where a staff member moves departments within the organisation, the previous line manager is responsible for revoking access to systems that are no longer appropriate for the new role.

The relevant business area must manage movers within the department.

Requests to the NHIS Service Desk must provide specific detail of the existing and amended access rights for the change to be actioned.

Employers of temporary staff, contractors and placements will request an account through the NHIS Service Desk. These accounts must be set with an expiry date, at which point the account will be disabled, unless NHIS is informed otherwise.

Where there is a possibility that a user will return after a long period of absence, the line manager can request re-enablement of the account.

IAAs can request a list of amended, leavers and starters to ensure access remains appropriate and staff moving post have their access revoked.

6.4. Removal (leavers) of User Access - Account Termination

It is the responsibility of a leaver's line manager to notify the NHIS Service Desk that a member of staff has left the organisation, and the account is to be disabled.

The organisation's Service Line Manager will institute a review of all system access rights for staff members at the exit interview or upon receipt of resignation notification. All physical equipment must be retrieved including laptops, phones, ID Cards, security tokens and other equipment provided by the organisation.

The request should be made in advance of the users last day and date to be disabled will follow the system's service level agreement deadline.

Access to third party services and assets (VPN) will all be disabled. The systems where shared passwords are implemented should be reviewed and passwords changed by the line manager (or IAO upon notification).

The email account will be disabled by the NHS mail Local Administrator (NHIS) and an Out of Office set up or divert, whichever is the most applicable.

For immediate termination or dismissal, the Service Desk must be informed by an authorised Senior Manager/Director by telephone to initiate immediate disablement of accounts.

List of leavers to be circulated to IAA's so accounts can be disabled.

6.5. Privileged Management

Privileged Accounts are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Holders of privileged accounts, such as system administrators, have privileges to perform most or all of the functions within an IT operating system.

The unnecessary allocation and use of special privileges are often major contributing factors to the vulnerability of breached systems

Access to systems must be relevant and commensurate with the business need of the organisation. That is, the minimum access that satisfies the business need must be given. Privileged access is used by individuals undertaking designated tasks within the job role and are only used for the purposes of system administration.

Privileged accounts must be authorised by the Information Asset Owner for the system, and where applicable, requested through the NHIS Service Desk for systems provided by NHIS. Access rights must be reviewed bi-annually as a minimum, by the IAO to ensure that they remain fit for purpose and access is withdrawn where the circumstances no longer warrant access.

Standard Operating Procedures must be developed for the system administrators for each of the applicable systems, setting out how housekeeping and regular review and proactive monitoring of accounts and when this will occur. A report must be forwarded to the IG Working Group (frequency to be agreed) as evidence that this has been undertaken and forms part of the annual report to SIRO.

A list of Do's and Don'ts for individuals who have been allocated a privileged account is cited in Appendix 3

6.6. Review of User Access Rights

Line managers or designated staff members must ensure that access to clinical and IT systems is reviewed and revoked for staff members transferring from their department or services.

A housekeeping report will be run on an agreed basis to ensure that user accounts are not being retained inappropriately. This will be undertaken by the system manager / Information Asset Administrator (IAA) or by NHIS under instruction by the Information Asset Owner (IAO). Any user account that cannot be positively identified as current must be disabled pending confirmation of deletion from the organisation employer. To allow for maternity leave and other periods of extended absence, status of users will be ascertained before permanent deletion of accounts.

The only exception to this will be where a line manager informs NHIS that the account should be retained, gives a reason why and has appropriate authorisation from Information Governance or the Senior Information Risk Owner (SIRO).

6.7. Deletion of Accounts

Accounts will initially be disabled on notification of a leaver or receipt of a leavers list from the organisation within an agreed period of the leaving date (this will be set out in the Standard Operating Procedure for the system). The accounts will be removed from all group memberships and generic accounts. NHIS Service Desk should be informed as soon as possible of organisation leavers to revoke access to patient identifiable data.
The accounts will be retained for an agreed time and then deleted permanently from the system. After this period, any data maintained by NHIS (including Home/G Drive) will be

deleted. Currently most clinical systems do not have a permanent delete option, as this would affect auditing/historic data. Accounts are just made inactive or archived.

The only exception to this will be where a line manager informs NHIS that the account should be retained, gives a reason why and has appropriate authorisation from IG or the Senior Information Risk Owner (SIRO).

6.8. Monitoring and Auditing of Inactive Accounts

Removal of inactive accounts is essential for the security of information systems. It may be preferable to retain accounts in disabled mode before deleting them permanently. If this is the case and has been authorised by the organisation, the password will be reset.

Access requests to NHIS by a leaver after the leave date but before the deletion date will only be granted upon appropriate authorisation from the employing organisation, such as IAA, line manager or head of department. Access will be granted for 7 days only.

Access request by a current staff member to an account belonging to an exited staff member will be granted depending on the business need and the appropriate written authorisation from the employing organisation, including Information Governance.

6.9 Zero Trust Security Principles

The Trust utilises a Zero Trust model for account management, ensuring that access is not granted solely on the basis of network location or device. All access requests are subject to ongoing verification, with the principle of least privilege enforced at all times. Segmentation and continuous monitoring are incorporated to further mitigate risks.

6.10 Third Parties

Third parties are required to follow the same account management standards as SFH users. Contracts involving third parties should specify breach notification procedures and grant audit rights. Remote access needs to be protected through VPNs and endpoint security checks, along with any other necessary controls.

6.11 Incident Response and Reporting

Any suspected account compromise must be reported immediately, in accordance with the Trust's Incident Management and Reporting Procedure.

7.0 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)**
Data Security Protection Toolkit	360 Assurance	Audit	Annually	Head of Data Security and Privacy/Audit and Assurance Committee/ Data Protection and Cyber Security Committee
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Working Group/Head of Data Security and Privacy/Audit and Assurance Committee/ Data Protection and Cyber Security Committee
IAO report to the SIRO	IAO	Self-assessment return	Annually	Head of Data Security & Privacy SIRO/ Data Protection and Cyber Security Committee

8.0 TRAINING AND IMPLEMENTATION

All staff must complete annual refresher training on Data Security & Awareness which covers account security, phishing and social engineering. All Privileged users such as Information Asset Administrators (IAAs), IAO's and those managing third party access must ensure that they undertake any role specific training associated with the asset that they manage and that any Information Asset Owners undertake risk assessments in line with organisational guidance.

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document has been subject to an Environmental Impact Assessment, see completed form at Appendix 2

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- NHS Digital exemplar Policy: Access control in health and care organisations
- NHS Digital – Secure Configuration
- NHS Digital - Identification and Authentication

Related SFHFT Documents:

- Information Security Policy
- Incident Management and Reporting Procedure
- Electronic Remote Access Policy
- Organisational Policy on Confidentiality

11.0 KEYWORDS

Information security, data security.

12.0 APPENDICES

- Refer to list in contents table

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Account Management and Access Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 23rd July 2024			
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	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion / Belief	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon 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.

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

Low Level of Impact

Name of Responsible Person undertaking this assessment:

Signature: G Robinson

Date: 23rd July 2024

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	No	
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example bunded containers, etc.)	No	
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No	
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No	
Energy	• Does the policy result in an increase in energy consumption levels in the Trust? (estimate quantities)	No	

Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	

APPENDIX 3 – PRIVILEGED ACCOUNTS GUIDELINES

Privileged accounts should be protected with the following controls:

DO

✓ Ensure that privileged users only use their system administrator account when elevated privileges are required. Their general user account should be used for all other work activities.

✓ Ensure that management or administrative access is limited to users who have been suitably authenticated and have been authorised to perform the specific action. Only those with a genuine business need should have an administrative account, however there should be a sufficient number of administrators that there is not a single point of failure due to absence or administrators leaving the Trust. This should be enforced through the principle of least privilege.

✓ Ensure that Multi Factor Authentication (MFA) is used where possible, such as where administrative consoles provide access to manage cloud-based infrastructure, platforms or services. MFA should also be used to access enterprise level social media accounts. Where MFA cannot be used on a system, this is considered an exception and should be logged in the risk register.

✓ Ensure that MFA is mandated for a privileged user to conduct important or privileged actions such as changing fundamental configurations including changing registered email addresses or adding another administrator.

✓ Ensure that MFA is used as a validation step, to confirm actions requested by users, such as a MFA re-prompt when attempting to delete or modify data.

✓ Ensure that default passwords are managed securely and safely, as described in the Password Management Policy

DON'T

✕ Allow privileged users to use their privileged accounts for high-risk functions. These include reading emails, web browsing, using an 'administrator' login on an end-user device (such as a mobile device), or logging into a server as 'root'.

✕ Leave default or factory set passwords for any accounts but particularly for privileged system accounts, social media accounts and infrastructure.

✕ Allow a user to have a privileged account, unless they are a system administrator and require a privileged account for that specific