Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

ACCOUNT MANAGEMENT AND ACCESS POLICY

POLICY

Reference	IG/012		
Approving Body	Cyber Security Assurance Programme Board		
Date Approved	29th September 2022		
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**
	✓		
Issue Date	April 2023		
Version	2		
Summary of Changes from Previous Version	Minor changes to text and update to formatting References to policy development through Cyber Security Assurance Programme with consultation across NHIS partners		
Supersedes	1		
Document Category	Information Governance		
Consultation Undertaken	Cyber Security Delivery Group Compliance Risk Assurance Management Meeting (NHIS) Information Governance Working Group (SFH) Nottinghamshire Integrated Care Board Nottingham CityCare Partnership -		
Date of Completion of Equality Impact Assessment	13/04/2022		
Date of Environmental Impact Assessment (if applicable)	13/04/2022		
Legal and/or Accreditation Implications	N/A		
Target Audience	All staff		
Review Date	September 2024		
Sponsor (Position)	Cyber Security Programme Board		
Author (Position & Name)	Cyber Security Delivery Group - Chair		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance / Information Security		
Position of Person able to provide Further Guidance/Information	Cyber Security Assurance Delivery Group		

Associated Documents/ Information	Date Associated Documents/ Information was reviewed
Information Security Policy	Not applicable
Template control	June 2020

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 docile, 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. Employees who leave the organisation or transfer departmentally can misuse their login credentials to access network resources.

1.2. The damage that can be done to the network depends on the skill of the intruder and how many privileges they have. 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 working 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. Also including all contractors, agency staff and third party.

2.0 POLICY STATEMENT

2.1. This document has been developed as part of the Nottinghamshire Health Informatics Service (NHIS) and partner commitments to maintaining a secure network as part of the Cyber Security Assurance Programme.

The Policy has been reviewed and developed by:

- Nottingham and Nottinghamshire Integrated Care Board
- Sherwood Forest Hospitals NHS Foundation Trust
- Nottingham CityCare Partnership

All partners are 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 general rule, IT systems shall be locked down 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 27001:2017 standard controls for management and monitoring of access controls.

Control Ref	Title
A.9.1.1	Access control policy
A.9.2.1	User registration and de-registration
A.9.2.2	User access provisioning
A.9.2.3	Privilege management
A.9.2.4	Management of secret authentication
A.9.2.5	Review of user access rights
A.9.3.1	Use of secret authentication information
A.9.4.2	Secure log-on procedures
A.9.4.3	Password management system
A.9.4.4	Use of privileged utility programs

2.5. This policy applies to all employees, 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)	User account management system
Accounts	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/
NHIS Intranet Site	http://intranet.nhis.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 employee is responsible for performing the tasks associated with initial registration, user change and 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 the systems provided by NHIS are responsible for reporting any breach of this policy to the appropriate manager via the incident reporting system Datix 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 Information Governance 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 Equality and Diversity Statement

6.1.1. SFH and NHIS aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

6.1.2. In carrying out its functions, SFH and NHIS must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which SFH and NHIS is responsible, including policy development, review and implementation.

6.1.3. Equality Impact Assessment screening has been completed on this policy and has identified no potential adverse effect for protected characteristic groups.

7.0 POLICY DETAILS

7.1. 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.

7.2. 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 on boarding 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, or by email to the NHIS.servicedesk@notts-his.nhs.uk

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 a valid business reason can be given 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 particular time unless a separate log is kept. It is also difficult to attribute particular 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.

7.3. Modifying/ Movers User Access

Where an employee 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 in order 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 can 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 in order to ensure access remains appropriate and staff moving post have their access revoked.

7.4. 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 employees 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.

7.5. 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. Examples of user accounts with privileges include administrative and super user accounts.

The unnecessary allocation and use of special privileges are often found to be a major contributing factor to the vulnerability of systems that have been breached.

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 at least annually 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.

7.6. 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).

7.7. 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 in order 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).

7.8. 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.

8.0 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)
IG toolkit validation	360 Assurance	Audit	Annually	IG Working Group/IG Manager/Audit and Assurance Committee/IG Committee
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Working Group/IG Manager/Audit and Assurance Committee/IG Committee
IAO report to the SIRO	IAO	Self-assessment return	Annually	IG Manager/SIRO/IG Committee

9.0 TRAINING AND IMPLEMENTATION

There are no specific training requirements associated with this policy. However, all Information Asset Administrators (IAAs) and IAO's must ensure that they undertake any training associated with the asset that they manage and that any Information Asset Owners undertake risk assessments in line with organisational guidance.

.

10.0 IMPACT ASSESSMENTS

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

11.0 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

APPENDIX I - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: ACCOUNTS MANAGEMENT AND ACCESS POLICY			
New or existing service/policy/procedure: Existing			
Date of Assessment: 13/04/2022			
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	None	None	None
Gender	None	None	None
Age	None	None	None
Religion	None	None	None
Disability	None	None	None
Sexuality	None	None	None
Pregnancy and Maternity	None	None	None
Gender Reassignment	None	None	None
Marriage and Civil Partnership	None	None	None

Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	None	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? • None			
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 (click here), please indicate the perceived level of impact: Low Level of Impact *(Delete as appropriate)* For high or medium levels of impact, please forward a copy of this form to the HR Secretaries for inclusion at the next Diversity and Inclusivity meeting.			
Name of Responsible Person undertaking this assessment: Jacquie Widdowson, IG Manager/DPO			
Signature:			
Date: 13/04/2022			

APPENDIX II – 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	