NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Account Management and Access Standard Operating Procedure for XXXXXXX

Document Category:	**Information Governance**
Document Type:	**STANDARD OPERATING PROCEDURE**

Keywords:	

Version:	**Issue Date:**	**Review Date:**
2	September 2023	September 2025

Supersedes:	1		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	29th September 2023

Scope/ Target Audience: (delete as applicable / describe)	**Trustwide**

Evidence Base/ References:	Information Asset Owner Framework

Lead Division:	Corporate Services
Lead Specialty:	Information Governance
Lead Author:	Jacqueline Widdowson, Head of Data Security and Privacy
Sponsor:	Sally Brook Shanahan, Director of Corporate Affairs

	Name the documents here or record not applicable
Associated Policy	Account Management & Access Policy Information Security Policy
Associated Guideline(s)	
Associated Procedure(s)	Password Procedure
Associated Pathway(s)	
Other associated documents e.g. documentation/ forms	

Consultation Undertaken:	Information Governance Working Group

Template control:	v1.4 November 2019

Contents

Purpose

The purpose of this procedure is to support the Information Security Policy and Account Management and Access Policy to provide a robust framework for the management of individual user accounts and access to Sherwood Forest Hospitals NHS Foundation Trust's, information assets, networks, and equipment. This procedure does not apply to generic accounts. However, a data protection impact assessment must be undertaken to ensure the use of generic accounts is appropriate. If a data protection impact assessment has been undertaken, the risk assessment section must be reviewed and updated where appropriate.

The procedure defines the processes that should be in place for granting, modifying, removing, and reviewing user access privileges to Trust systems, in order to protect the confidentiality, integrity and availability of confidential information.

Information Asset Owner	Insert name here
Information Asset Administrator	Insert name here

Policies

Information Security Policy[1]

Account Management and Access Policy[2]

Summary of Roles and Responsibilities

Roles	**Responsibility**
IAO - Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.	Will have overall accountability of the information asset. Will approve and present the annual report to SIRO to provide assurance on the information asset.

[1] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8640

[2] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618

IAA - Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.	Will comply with User Access Management procedures for their information asset. Are responsible for ensuring third-party service providers of services and systems comply with User Access Management procedures. Are responsible for retaining a record of user access requests, approvals, terminations, and disabling for information assets for auditing purposes. Are responsible for documenting and retaining a record of user access reviews for auditing purposes. Will compile the report to SIRO and forward to the IAO for approval.
All staff including Medirest, Skanska, agency, suppliers and contractor colleagues	Are responsible for the protection of their individual account and password, must not share their password with anyone, or allow others to use their account in accordance with the information security policy Will immediately change their password and/or notify IAA if they believe their account details have been disclosed or used by an unauthorised user. Will log out of their account or use screen lock when not present to prevent unauthorised access to their account
Administrator – will usually have elevated access rights to the system in addition to a standard account	Are responsible for the protection of administrator account details and must not share administrator account details with unauthorised users. Will immediately change the account password and notify the IAA of the relevant information system if they believe an administrator account has

	been improperly disclosed or used by an unauthorised user. Will only use administrator accounts for performing administration related duties and not business as usual activity. All non-administrator activities must be performed under the employee's standard user account.

Granting User Access

Access to confidential information will be provided on a need to know basis and to those who have a legitimate need for the information.

The principle of least privilege must be adopted that users and applications should be granted access only to the data and operations they require to perform their jobs.

Access to insert system name here will be granted based on (RBAC or similar, how do you determine access)

Requests for access to insert system name here are forwarded to the IAA/IAO who is responsible for approving new or amended requests for user access.

Third-party service providers must comply with the User Access Management Procedure and ensure that user access to information systems and data is granted only for individuals that have been authorised by the relevant IAO/IAA.

Modifying/ Movers User Access

Where an employee moves departments within the organisation, the previous line manager is responsible for revoking access to systems.

IAA's will ensure that when an employee changes role within the organisation, their access will be amended so that it reflects the requirement of their new role via the new line manager.

Any user access privileges to insert system name here information systems or services that are no longer required for the employee's new role will be removed.

Requests for changes to an individual's user access privileges for a system are to be forwarded to the IAA.

IAA /IAO is responsible for approving changes to user access for information systems.

Removal (leavers) of User Access - Account Termination

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

Employees that are leaving, for any reason will have their user access disabled at the end of their employment unless an exemption is granted by the IAO.

Administrators will remove application specific access for the user account.

Suspension of User Access

The Trust reserves the right to revoke the system privileges of any user at any time.

Reviewing User Access

IAA’s will conduct a user access review every decision how often the access to systems to be reviewed months (3 months as a maximum) to ensure that current access to systems and services are relevant and appropriate for individual users.

IAA’s are responsible for conducting annual user access reviews of permissions within their department's information assets.

User access reviews should be documented and retained for auditing purposes.

Changes to user access for an information system identified as part of user access reviews should be performed by following the relevant procedures for modifying or terminating user access privileges.

IAA’s to create their own specific procedures to review user access accounts for their system and to have a documented procedure in place.

Administrator Account Management (Privileged Accounts)

Administrator account details will only be disclosed to individuals who require this type of access based on their role.

Where possible, default administrator accounts for information systems should be disabled. If the account cannot be disabled, the account should be renamed and the default password should be changed immediately.

Requests for access to an administrator account must be authorised by the IAO.

Administrator accounts must only be used for performing administration-related activities. All non-administrator activities must be performed under the employee's user account.

Passwords for administrator accounts must be changed at least to decide how often password needs to be changed (6 months as a maximum) or immediately if a user with knowledge of the password leaves the Trust or no longer requires access to the account based on their role.

Administrator account access is to be reviewed at least to decide how often these need to be changed.

Contractor/ Temporary Account Access

Contractors/ Temporary access will be assigned to a user account for temporary access to information systems this will be set to expire according to the expiry date agreed.

Contractor/ Temporary user accounts will be terminated within the specified timeframes

Administrators/ IAA are responsible for removing application specific access for the account.

Any contractor/ temporary user account that has been inactive for a period of to decide inactivity period (3 months maximum) days or more will be disabled.

Report on Access Controls

A report on the access controls in place for the insert system name here will be provided by the IAO annually as part of the annual report to SIRO.