Sherwood Forest Hospitals
NHS Foundation Trust

Template - Account Management & Access Standard Operating Procedure for XXXXXXX

Document Category:	Information Governance
Document Type:	STANDARD OPERATING PROCEDURE

Keywords:	

Version:	Issue Date:	Review Date:
1	03/ 09/2021	03/09/23

Supersedes:	N/A		
Approved by (committee/group):	IG Committee	Date Approved:	July 2021

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

Evidence Base/ References:	

Lead Division:	Corporate Services
Lead Specialty:	Information Governance
Lead Author:	Jacqueline Widdowson, Data Protection Officer & Information Governance Manager
Sponsor:	Shirley Higginbotham, Director of Corporate Services

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

Consultation Undertaken:	Information Governance Working Group

Template control:	v1.4 November 2019

CONTENTS

Contents

Purpose

The purpose of this Account Management & Access Standing Operating Procedure is to support the Information Security Policy and Account Management and Access Policy and provide a robust framework for the management of user access to Sherwood Forest Hospitals NHS Foundation Trust, information systems, networks and equipment.

The Account Management & Access Standard Operating Procedure defines the procedures in place for granting, modifying, removing, and reviewing user access privileges to SFH systems in order to protect the confidentiality, privacy and security of SFH information assets.

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

Policies

Information Security Policy Sherwood Forest Hospitals (sfh-tr.nhs.uk)
Account Management & Access Policy Sherwood Forest Hospitals (sfh-tr.nhs.uk)

Summary of Roles and Responsibilities

Roles	Responsibility
IAO	Will have overall accountability of the system. Will approve and present the annual report to SIRO to provide assurance on the information asset.
IAA	Will comply with User Access Management procedures for their information system. Are responsible for ensuring third-party service providers of services and systems comply with SFH User Access Management procedure. Are responsible for retaining a record of user access requests, approvals, terminations, and disabling for

	information systems 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.
Employees, contractors, temporary/ 3rd party	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	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

Granting User Access

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

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 *induvial who will authorise request,* who is the responsible *IAA/IAO* who is responsible for approving new 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

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. 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 to be forwarded to *name of IAA.*

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

Removal (leavers) of User Access - Account Termination

Employees that are leaving SFH, 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 at a minimum to ensure that current access to systems and services are relevant and appropriate for each individual user.

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* 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* 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 annually as part of the annual report to SIRO