Shropshire Community Health NHS

NHS Trust

Policies, Procedures, Guidelines and Protocols

Document Details	
Title	**Finance Procedure Y2: Oracle Username & Password Control**
Trust Ref No	827-56175
Local Ref (optional)	
Main points the document covers	How Oracle usernames and passwords are used and controlled
Who is the document aimed at?	All staff
Author	David Court, Head of Financial Accounting
Approval process	
Approved by (Committee/Director)	Director of Finance
Approval Date	August 2022
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Sarah Lloyd
Category	Finance
Subcategory	Finance Procedures
Review date	August 2025
Distribution	
Who the policy will be distributed to	Distributed to senior staff as defined by Directors
Method	Electronically to senior staff & available to all staff via the Trust website
Document Links	
Required by CQC	
Required by NHS Resolution	
Other	

Amendments History		
No	Date	Amendment
1	August 2013	Additional details on passwords & remove references to PCTs
2	August 2016	Minor changes to terminology
3	August 2019	Added in 6.2 automated checks for users not using system in last 12 month. Changed ‘System Admin team’ to ‘System Administration team’
4	August 2022	No Changes Required
5		

1 – Introduction

1.1 The Oracle applications suite is used by the Trust for General Ledger, Accounts Payable, Accounts Receivable, Cash Management, Internet Procurement, Purchasing and reporting operations. The system allows for password restricted access at responsibility, menu, and process level.

1.2 This procedure covers: –
- a) user access – usernames and passwords
- b) issue of new or replacement usernames and passwords
- c) end dating usernames and employees
- d) access rights – considerations.

2 – Usernames and passwords

2.1 A single Oracle database instance exists which supports multiple sets of books. Each set of books relates to a distinct business organisation. There is therefore a set of books for the Trust (as well as one each for the 2 Acute Trusts).

2.2 In order to login to Oracle, a user requires a username that identifies them within the system, a responsibility that defines their general role and an employee record in their respective set of books should they have a requisitioning or purchasing role. Associated with this username is a password.

2.3 Staff in Systems Administration roles have responsibilities that relate to multiple sets of books. The username is in the form of the users first initial, and surname followed by 01 for the first user with this combination and 02, etc. thereafter and CT as an organisation identifier suffix.

2.4 Passwords can be set to expire after a number of logon attempts or after a number of days. This is set to 30 days. Once a password is changed the next user logon initiates the change of this password so a System Administrator will not know a user’s password.

2.5 At any time after their initial login, the user may change their password by selecting Notifications, then Preferences, then Change Password. Passwords must be alphanumeric and consist of at least 8 characters with no repeating characters.

2.6 The “Login Assistance” link on the Oracle log-on screen has functionality to allow users to automatically re-set their password if it is lost or forgotten. An email is automatically generated from Oracle to the email address associated with the user. Alternatively, any local system administrator can manually re-set a user password.

3 – Control of logins

3.1 Only Sysadmin Responsibilities can create new usernames, and these must be associated with an employee. Employee records are set up by local systems leads within each Trust and the username by the centralised Systems Administration team, hosted by Shropshire Community Health NHS Trust.

4 – New user setup

4.1 When a new username is required, the appropriate manager requests the local systems lead (usually via e-mail) to establish a new employee record in the Purchase Order responsibility – this is done even if the user only has Finance responsibilities, and not Purchasing ones. The required details are then forwarded to the Systems Administration team to set up the username and password.

4.2 The employee record is checked against the ESR payroll system where the new user is an employee. Where the employee is to have delegated authority to approve requisitions/invoices this is checked against the Authorised Signatory Database (ASDB) to ensure that a correctly completed signatory form is in place, signed off by a Budget Holder.

4.3 Once a user has been set up, they are linked to Responsibilities. Most users are internet procurement users and therefore only have that one Responsibility. Finance users can have several as they usually require access to more than one Oracle sub-ledger. Section 5 below gives more detail on this. A report to check Responsibilities assigned to users is run by the Systems Administration team on an annual basis to ensure no errors have been made or changes not actioned.

4.4 Once usernames and responsibilities are set up, a password is created for the user and an e-mail notification is sent to them informing them of the required details.

5 – Allocating responsibilities to users – general principles

5.1 Within Oracle, access rights are allocated to Responsibilities. A Responsibility may be assigned to a single user or a number of users with similar access requirements. These responsibilities are agreed between the Finance Department Section Heads and the Systems Administration team and are devised to enable access by the users to system facilities in accordance with Standing Financial Instructions and finance procedures.

5.2 The Finance Department has a requirement to segregate related duties, and the Responsibilities reflect this. There is no definitive allocation of rights, but administration/control issues and separation of duties must be taken into account. In particular: -

a) access to the Sysadmin Responsibility is for the Systems Administration team and local systems leads only

b) access to periodic processes should be restricted to nominated senior officers

c) users working in the Discoverer reporting environment can only run reports and cannot amend existing ones

5.3 In addition to the above, requirements will alter from section to section and with the job descriptions and seniority of individual staff. Each case should be carefully considered on its merits.

6 – End dating an existing user

6.1 When a username is no longer required (i.e., a user leaves or changes job) it is the responsibility of that user's manager to notify (preferably by e-mail) both the Systems Administration team and the IM&T helpdesk. The Systems Administration team ensure that the username is end dated. IM&T ensure that access to the user's local files is passed to their immediate superior, or Head of Department.

6.2 Additionally quarterly reports are run from ESR to identify and end date leavers who have not been notified to the Systems Administration team, as well as an automated check for anyone who has not used the system in a 12-month period.

References & associated documents

Authorised Signatory Database

Reviewed By ______________________ Date ___________________

Authorised By ______________________ Date ___________________