POL010 User Account Management Policy

Version	**1.1**
Ratified By	Integrated Governance Board
Date Ratified	June 2018
Date of Issue via Intranet	August 2018
Date of Review	**June 2019**
Lead Officer	**Ian Hart**
Executive Lead	**Debbie Bywater**

Contents

Information Reader Box	
Directorate	
Communications & Engagement	Information Technology
Continuing Healthcare	Corporate Affairs
Contract Management	Business Intelligence
Finance	Human Resources
Publications Gateway Reference	xx
Document Purpose	Policy and High Level Procedures
Document Name	IT User Account Management Policy
Author	Information Technology
Publication Date	June 2017
Target Audience	All CSU Employees
Additional Circulation List	n/a
Description	Policy for defining IT User Account Management
Cross Reference	n/a
Superseded Document	n/a
Action Required	To Note
Timing/Deadlines	n/a
Contact Details (for further information)	Ian Hart, Assistant CIO 1829 Building Countess of Chester Health Park Liverpool Road Chester CH2 1UL Ian.Hart@nhs.net 01244 650546

-

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

1 Introduction

Effective security controls in relation to access to data are an essential component of the effective risk management of all Information Systems . Access controls protect information by managing access at all entry and exit points, both logical and physical.
These measures ensure that only authorised users have access to specific information, systems and facilities. User accounts offer a way of managing access, providing user accountability and tracking use of information, information systems and resources.
User accounts can take various forms from a system login to an ID swipe card. Therefore the application of access controls, the management of user accounts and the monitoring of their use plays an important part in the overall security of information resources.

1.1 Purpose of Policy

To establish consistent guidelines for the management of user accounts within the MLCSU data infrastructure and associated Information systems.

1.2 Scope of this Policy

The scope of this policy includes to all staff of Midlands and Lancashire CSU (MLCSU) or who have Application System Manager or equivalent rights to any of the IT systems in use with the MLCSU.

An Application System Manager defined as any role that hold administration permissions to one or more IM&T systems and is responsible for access security, password management etc.

1.3 Aim of this Policy

The main aims of this policy are:

- To make employees of the Midlands & Lancashire CSU aware of their responsibilities regarding User Account Management
- To ensure that all employees are fully aware of and comply with the process and procedures bound to this policy.

2 Policy Statement

2.1 Why Do We Need User Account Management?

In order to help maintain the security and integrity of the Trust electronic systems it is imperative that every system -whether accessed via local desktop PCs, communication networks and equipment, or larger systems machinery contains appropriate mechanisms for ensuring that only authorised users may gain access to information, programs, files and databases. Systems must be protected against a variety of threats. Every system must be able to identify any user who justifiably requests access to it and repel all unauthorised intrusion, whether accidental or malicious. Equally, every system must ensure that even authorised users are only given access to those areas which they require in order to complete their working duties. Much of this control will be maintained by the use of user accounts and passwords.

2.2 Summary of Responsibilities applicable to All MLCSU Employees

It is essential that all Midlands & Lancashire CSU employees are familiar with their own responsibilities for ensuring that the this policy is followed.

2.3 Awareness and Understanding

It is essential that all key stakeholders as stated in this section are familiar with the contents of this policy so that they can understand and carry out their responsibilities. The responsibilities of particular users in assuring awareness and understanding are laid out in this section.

2.3.1 Application System Manager

- The creation, suspension and deletion of user accounts are the responsibility of the Application System Manager or their designated deputy(s).
- User accounts must not be requested by the individual user but can be requested their supervisor or manager using relevant form for their area or where a smartcard is required via form RA01
- The Application System Manager should retain a copy of these requests for audit purposes.
- All user accounts should be clearly identifiable by the user's roles and responsibilities.
- Only those accounts which are required to write data to the information system shall have that function. All other users will have a read only function.

- The Application System Manager must maintain a list of all staff that have been granted Application System Manager or equivalent rights.
- Suppliers and support companies must have their own user accounts set up, the MLCSU password management policy will apply to these accounts.

.

2.3.2 Human Resources

- The HR department will create on a monthly or more frequent basis a report of leavers within the MLCSU
- This report will be forwarded to the MLCSU Service Desk who will use the report to verify that all leaver accounts have been suspended.
- If an account is found to be still active after the date of termination then the Information Security Team and all relevant Application System Manager's shall be informed via MLCSU Service Desk

2.3.3 Role of Supervisor / Manager

All supervisors / managers are responsible for informing the MLCSU Service Desk and the relevant Application System Manager(s) of the following:-

- New Starters – start date and role
- Leavers – leaving date
- Long term sickness – date off work
- Maternity leave – date leave commences
- Movements – where by doing so the user needs differing system access

2.3.4 Role of IT Service Desk

- The IT Service Desk manages user accounts for Active Directory services.
- The creation, suspension and deletion of these user accounts is the responsibility of the MLCSU Service Desk
- User accounts must not be requested by the individual user but can be requested their supervisor or manager using the CSU All in One Form
- The MLCSU Service Desk should retain these requests for audit purposes.

- All user accounts should be clearly identifiable by the user's roles and responsibilities.

2.4 **System-level Passwords**

All system-level passwords (e.g., root enabled, Administrator, application administration accounts, etc.) must be changed every 28 days.

It must also be changed whenever a change in Application System Manager / Administrator occurs.

User-accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

The Application System Manager must maintain a list of all staff that has been granted System Manager or Administrator rights.

2.5 **Account Housekeeping**

Authorised Application System Managers should periodically check that all user accounts are still in use. If an account has not been accessed for 28 days then the account may be suspended until either HR or the user's departmental head has been contacted.

2.6 **Compromised Accounts**

If an account or password is suspected to have been compromised, report the incident to the MLCSU Service Desk who will in turn inform the Information Security Manager. Such passwords will be suspended immediately and until the password is changed

2.7 **Password / Pin Security (All Users)**

A password must be at least eight characters long and not relate to the user's name or system account.

Passwords must not be written down or inserted into email messages or other forms of electronic communication.

All passwords must be changed after the initial login and then changed on a regular basis with a maximum of 90 days.

Password changes should be unique from previous passwords on systems that support this feature.

To prevent password guessing, logon accounts should be configured to lock out after six unsuccessful attempts on systems that support this feature.

3.0 Internal Process

MLCSU will receive instructions to undertake a number of internal administration tasks from different departments, these are summarised below:-

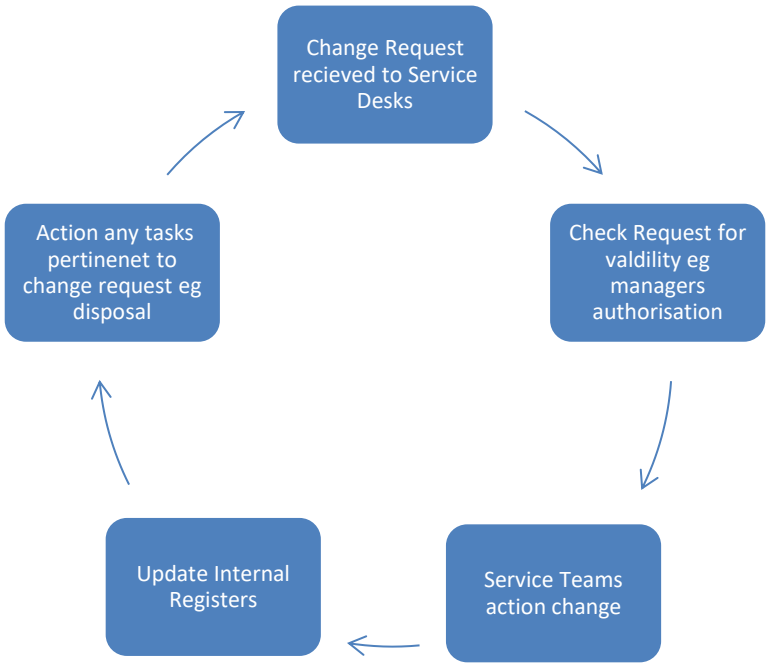
- Starter Request
- Leaver notification
- Change in role notification
- Request for change (eg grant or remove rights to system access, file shares etc..)

Each of the above tasks will require MLCSU IT department to process the requests as stipulated by the associated documentation and standard forms.

It is important to note that currently each geographical health economies operate different forms and processes and this is due to local infrastructure.

MLCSU are currently reviewing internal processes with a view to further standardise the process and forms that to be used in the future.

Overview of Process



The above process outlines key processes that are undertaken during the normal lifecycle of requests coming to our service desk

- Change Request: change request can be a number of different tasks outlined below
    - New user form that requires NHSmail, local AD accounts, access to a number of MLCSU internal systems e.g. Tallypro, Wordpal, Broadcare,
    - Leavers form, suspend NHSmail account, disable AD account, retrieve IT equipment
    - Request for New equipment
    - Amendments to access rights

- Check Request for Validity: service desk to check forms have been correctly completed and the appropriate authorisation is valid

- Service action Change: Once the request has been logged the change request will be sent to the appropriate support queues for action e.g. if access rights need change this request is sent to the 3rd line teams

- Update Internal Registers: documents and update any internal registers to reflect change, e.g. call in Sunrise, update asset registers

- Action any other Task related to change request: action any other tackles related to the change request such as secure disposal of equipment, receipt of equipment and arrange re-image

The above standard process is to be used by MLCSU staff however as outlined below a number of different forms are currently used based on local infrastructures:-

3 Scope

3.1 Officers Within the Scope of this Document

3.1.1 Officers who does this Policy Apply to?

- Midlands & Lancashire CSU Employees.
- Employees and Agents of other organisations who, may seek to deploy/change/decommission assets belonging to Midlands & Lancashire CSU and its customers.
- Midlands & Lancashire CSU Client Organisations/Client Nominated Representatives.

3.2 Officers Not Covered by this Document

3.2.1 There are no Officers of Midlands & Lancashire CSU (Information Technology) not covered by this document.

4 Corporate Level Procedures

4.1 **Sub-heading on contents page**

4.2 Sub-heading not on contents or paragraph text

5 Distribution & Implementation

5.1 Distribution Plan

5.1.1 This document will be made available to all Officers via the Midlands & Lancashire CSU internet site.

5.1.2 A global notice will be sent to all Officers notifying them of the release of this document.

5.2 Training Plan

5.2.1 A training needs analysis will be undertaken with Officers affected by this document.

5.2.2 Based on the findings of that analysis appropriate training will be provided to Officers as necessary.

5.2.3 Guidance will be provided on the intranet site.

6 Monitoring

6.1 Compliance

6.1.1 Compliance with the policies and procedures laid down in this document will be monitored via the IT Strategy Board together with independent reviews by both Internal and External Audit on a periodic basis.

6.1.2 Debbie Bywater, in conjunction with the Chris Knight, is responsible for the monitoring, revision and updating of this document.

6.2 Equality Impact Assessment

6.2.1 This document forms part of Midlands & Lancashire CSU's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

6.2.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

7 Associated Documentation

All in one form - CSU staff_December 2016

8 References

n/a

Appendix 1 Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
0.1	June 2017	Ian Hart	DRAFT	
1.0	June 2017	Ian Hart	Approved	
1.0	December 2017	Ian Hart	RATIFIED	Integrated Governance Board

Appendix 2 Definitions

Unless a contrary intention is evident or the context requires otherwise, words or expressions contained in this document shall have the same meaning as set out in the National Health Service Act 2006 and the Health & Social Care Act 2012 or in any secondary legislation made under the National Health Service Act 2006 and the Health & Social Care Act 2012 and the following defined terms shall have the specific meanings given to them below:

CSU Executive	means the Managing Director and Executive Members collectively as a body.
Budget	means a resource, expressed in financial terms, proposed by the CSU Executive for the purpose of carrying out, for a specific period, any or all of the functions of the CSU.
Clinical Commissioning Group/CCG	means a body established in accordance with section 1I of the NHS Act 2006.
Employee	means a person paid via the payroll of Midlands & Lancashire CSU.