Approved Sept 2020

North West London
Collaboration of
Clinical Commissioning Groups

ICT
Procedure for Managing and Granting Active Directory Privileged Accounts

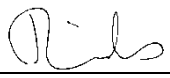
Version: 2.0

Version Control

Version Number	Reviewing Committee / Officer	Date
1.0	NHS NW London Clinical Commissioning Group, IT Security & Cyber Security Team	01/03/19
1.1	Altaf Suleman (ICT Security Officer) – Amended reviewers and approvers	28/08/20

Reviewers

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Abhilash Abraham		Head of IT & Cyber Security	02/09/2020	1.1
Ernest Norman-Williams		NWL GPs - Data Protection Officer		
Felicia Ayo-Ajala		Corporate Data Protection Officer		
Jenny Greenshields		CFO/SIRO	21/09/20	2.0

Approvals

This document must be approved by the following:

Title	Signature	Title / Responsibility	Date	Version
Jenny Greenshields		CFO/ SIRO	21.09.20	2.0
NWL CCGs Governing Bodies	----------	NWL CCGs Governing Bodies	Sept 2020	

Contents

If being read as a paper copy, please refer to ICT Department Section on the NWL Shared Services ICT intranet to ensure this is the current version

1. Introduction

- System and database administrators/managers will typically have special system access rights that allow them to view and correct data as part of a system's maintenance, monitoring or potentially to make amendments as a result of other users errors. This constitutes the basis of privilege management i.e. privileged users or super-users.

- In line with the National Cyber Security Centre 10 Steps to Cyber Security the NWL Shared Services ICT acknowledges the importance of ensuring there is a structured authorisation process for managing uses privileges.

- If users are provided with unnecessary system privileges or data access rights, the risk and subsequent impact of misuse or compromise is significantly increased.

- This could lead to:-

  The misuse of privileges where users accidentally or deliberately abuse the level of privileges they have been granted resulting in either the user themselves or a 3rd Party having unauthorised access to information or making unauthorised system changes that may directly impact security or business operations.

  Increased attacker capability where attackers take the opportunity to use redundant or compromised accounts to carry out attacks and possibly sell access to others.

  Negating established security controls where attackers have privileged system access they may make changes to security controls to enable further attacks or might attempt to cover their tracks by changes to audit logs.

- Such accounts should be kept to a minimum and the actions of those using the accounts identifiable, auditable and accountable.

- Access should be on a need to know basis. Users should only ever be granted the level of access and privileges that they need in order to carry out their duties (least privilege),

- The granting of highly elevated system privileges should be carefully controlled and managed and should be done via a Change Management Process.

- Users who are granted privileged accounts must understand their responsibilities to ensure the confidentiality, integrity and availability of the systems they have access to, and to act only within the scope of the access they have been granted.

2. Purpose and Scope

- The purpose of these procedures is to ensure there is a controlled authorisation process for registering and de-registration users who require a privileged account status, an account deemed higher than that of a standard user.

- For users granted these special privileges to understand their responsibilities towards the use of such privileges and the consequences of their misuse.

- This procedure therefore extends to:-

- Enterprise Administrators
- Domain Administrators
- Local PC Administrators

3. Procedures for granting privileged accounts

- All requests for privileged accounts that include Enterprise, Domain, and Local System Administration must be documented through the ICT Change Control process and therefore only authorised as part of that process by those with authority of that ICT group. This will provide assurance that no one person can act on the NWL Shared Services ICT's behalf in authorising privilege accounts.

  In order to allow the correct evaluation of the request, the ICT Change Control form should be completed and submitted for review with full details that include:-

  - Name, Job Role and contact details of the person requesting the access.
  - Name, Job Role and contact details of the person the access is to be granted for.
  - Level of access required.
  - What the access will apply to.
  - The reason for the request.
  - The length of time the access is required for.
  - Confirmation that if access is granted they will sign and abide by the ICT Code of Conduct for Privileged Accounts outlined in Appendix 1. (This must be in place before the account will be activated.)

- If the relevant information required to make the decision is not present on the Change Control Request will be returned to the requestor for re-submission.

- Users will only be granted the reasonable minimum rights and permissions to systems, services and information that they need to fulfil their business role.

- Users must set passwords in line with (CCG) Policy. Users are responsible for using strong passwords.

- Where the password policy is deemed to be impractical this needs to be documented as part of the change control procedure and the reason given so that it can be considered at the review stage. The Change Control Board will make any decisions relating to this.

- Staff authorised for Enterprise and Domain accounts MUST NEVER use the account for high risk or day to day user activities such as Internet use/web browsing or for emailing. Actions on these accounts must only be used to undertake the appropriate action required at that time, with the user immediately reverting back to their own standard account for their day to day activities.

3.1 Activation of authorised accounts

- If the request is authorised, it will not be activated until the (note relevant team) have received the completed Code of Conduct for Privileged Account form via email. This must be emailed to:- (note relevant email). A copy of this will be attached to the relevant Change Control Request so that an audit trail is maintained.

3.2 Staff Awareness

- Staff will be asked to sign the form as outlined in Appendix 1 to demonstrate their understanding of their responsibilities and expected code of conduct in the use of privilege accounts. Forms must returned to (note relevant email) via the users NHSmail email address.
- Forms will be retained as a record and held for access auditing purposes.
- Staff reminders for ensuring appropriate use of these accounts will form part of the (note relevant team) staff awareness circulars.

3.3 Auditing, Monitoring and Review

- Authorised accounts will be monitored by ICT Department through the (note relevant team).

- This procedure will form part of the annual audit programme conducted by the (note relevant team) to ensure principles outlined in it are being adhered to.

- This procedure will be reviewed every three years to ensure it remains fit for purpose and up to date, or sooner if changes in service, guidance or legislation dictate.

3.4 Inactive Accounts

- Accounts that are inactive for three months will be de-activated by the (note relevant team).

3.5 Revoking Accounts

- The ICT Department reserve the right to withdraw privilege access at any time without notification if it is deemed that patient care or the security of the NWL Shared Services ICT is or could be put at risk as the result of the actions of a user.

3.6 Disciplinary

- If it is found that staff operate outside of the scope of the authorisation granted to them without the prior authorisation of (note relevant senior level) level it will be viewed as a disciplinary offence.

3.7 Associated Documents

- (note relevant documents)

3.8 References

- National Cyber Security Centre – 10 Steps to Cyber Security
- NHS Digital – Data Protection and Security Requirements

Appendix 1

Code of Conduct for the Use of Privileged Accounts

This Code of Conduct **MUST** be returned to the (note relevant team) email (____) via your NHSmail email address to confirm that you understand and agree to the responsibilities as a "Privilege" account holder. The authorised account will not be activated until the signed form is received. The form will be held by the (note relevant manager)/attached to the Change Control Request and will be made available for audit.

1. I understand that the account I have been provided with is for my use only and must not be divulged to anyone else.

2. I understand that any abuse of access will result in the immediate de-activation of my account without notification, and could result in the permanent withdrawal of access and/or disciplinary procedures being taken against me.

3. I must operate only within the access I have been granted for the purpose I have been authorised.

4. If by default my access provides me with the ability to access areas outside the scope for which I have been authorised, it will be seen as a misuse of privilege if I deliberately act on this.

5. If I become aware during my duties of any additional access I have been inadvertently granted outside the scope of the original request I will advise my Manager and the (note relevant security manager role) immediately.

6. I understand I have no authority to grant myself or anyone else access to a privileged status account and any such requests must go through the ICT Change Control process.

7. If I become aware of any risks associated with my access I will inform both my Manager and the (note relevant security manager role) immediately.

8. I will ensure my password is a strong password in line with the NWL Shared Services ICT (note relevant policy), is kept secure, never shared or revealed regardless of whether with a colleague, line manager, system support staff or otherwise and managed/changed in line with the Policy.

9. If at any time I believe my account has been compromised I will immediately advise my manager and the (note relevant security manager role) via the NWL Shared Services ICT (note relevant email).

10. I will ensure any incidents (or near misses) relating to my password are logged to the (note relevant system) Incident Management system.

11. I will ensure that I notify both my manager and the (note relevant security manager role) if I no longer require the access provided whether that is as a result of the duties no longer failing within my remit, a change of role within the NWL Shared Services ICT or by leaving the NWL Shared Services ICT.

12. If I hold an Enterprise account that allows me full access to the NWL Shared Services ICT Network and Systems, I will never under any circumstances use it as a business as usual account**.**

13. If I need emergency access to an area of the network or system outside of the scope of the original authorisation I must seek additional authorisation from (note relevant role at Director/Assistant Director level in IT) who will follow the emergency Change Control Procedure.

14. I accept that all my actions as a privilege user are subject to auditing and monitoring.

I the undersigned confirm that I have read, understood and accept the responsibilities outlined in all 14 points in this Code of Conduct and will abide by them all as part of the role I have as a holder of an account considered a privileged account. I agree to act responsibly to ensure the security, confidentiality, integrity and availability of the information and systems I have access to.

Name
Job Role
NWL Shared Services ICT NHSmail Email
NWL Shared Services ICT Contact Number
Signature
Dated
For ICT USE ONLY **Date Form Received**