## Elevated Privilege Procedure

### PROCEDURE SUMMARY
This document is designed to control the processes in place that govern the procedures for the assignment of elevated privilege (admin) accounts within Active Directory (AD).

### The Trust monitors the implementation of and compliance with this procedure in the following ways:
Regular monitoring by IT Service personnel.

### Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Essex MH&amp;LD</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>CHS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
1.0 INTRODUCTION

2.0 NAMING CONVENTION

3.0 PASSWORD CREATION

4.0 ADMIN GROUPS

5.0 ADMIN GROUP MEMBERSHIP

6.0 REVIEW

7.0 REFERENCE OTHER DOCUMENTATION
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Elevated Privileges Procedure

Assurance Statement

This policy provides assurance to the following requirements laid out by NHS Digital to comply with the Cyber Essentials Plus requirements –

System administrative access privileges are restricted to a limited number of authorised individuals. Individuals should only have administrative access to those areas required to do their job.

1.0 INTRODUCTION

1.1 Admin or elevated privileges accounts within Active Directory (AD) can allow for changes to be made to users, endpoints, servers, domains and files.

1.2 The purpose of this document is to provide a description on how ICT Services assign new accounts with elevated privileges relative to their assigned job role.

1.3 This procedure should be followed by all ICT staff responsible for creating accounts with elevated privileges.

2.0 NAMING CONVENTION

2.1 All Admin accounts will only be created by members of the Cyber Security Team. Any request for a new admin account is to be logged on Richmond and passed to the Cyber team to action and must follow the process outlined in the Admin Accounts Procedure.

2.2 The following naming convention will be used when creating new admin accounts within AD:

adm. – First initial of first name – First five letters of surname

For example the user John Smith will be – adm.jsmith

2.3 Elevated accounts must not be used as the user’s primary account.

3.0 PASSWORD POLICY

3.1 Unique password will be created and used by individuals when performing administrative functions.

3.2 Passwords set for admin accounts should not be set the same as any existing accounts for any other systems (separate passwords for email accounts, network logins and any access to additional systems).
3.3 As best practice, passwords created for admin accounts should be created using the following format:

- A minimum of 12 characters long.
- Contain uppercase letters.
- Contain lowercase letters.
- Contain numbers.
- Contain special characters or non-alphanumeric characters, such as - ! " £ $ % & * @

3.4 All admin accounts will set to automatically force a password change every 30 days, admin account passwords are required to be changed every 30 days in compliance with the Data Security and Protection Toolkit.

3.5 No passwords should be repeated within 36 months.

4.0 ADMIN GROUPS

4.1 New elevated accounts will be placed in a marked organisational unit (OU) in the domain titled Admin Users within Active Directory (AD).

4.2 New elevated accounts are to be added to the AD groups that provide the required elevated rights as per below (these are the core groups, accounts may be placed in additional groups not listed below) –

- Server Administrators – Members of this group role will have local administrator access to servers.
- UEPR Servers – Members of this group role will have access to the identified UEPR Servers, for example the Mobius Dev environment and the HIE servers.
- File & Print Servers – Members of this group role will have access to the identified Service Delivery Servers, for example access to File and Print Servers as well as Safeboot.
- Local Administrators – Members of this group role will have local workstation admin access on endpoint devices.
- AD Object Management – Members of this group role will have access to create user and computer accounts within AD.
- Password Reset Delegate - Members of this group will have access to reset Domain User account passwords.
- Domain Admins – Members of this group will have complete control over all domain controllers and all directory content stored in the domain, including users, computers and group policies. Members can also modify the membership of all administrative accounts in the domain.
5.0 ADMIN GROUP MEMBERSHIP

5.1 Admin accounts will be granted access based upon the identification of which job role the user will be operating under.

5.2 Should any additional job functions be identified the new administrative account will be added into the appropriate security groups granting access to only the required level of access.

5.3 Admin accounts will be granted access to one or more security groups depending upon the job role.

- **Contact Centre** – Access granted to Password Reset Delegate security group
- **IT Trainers** – Access granted to Local Workstation Administrators and AD Object Management security groups
- **SystmOne** – Access granted to Local Workstation Administrators
- **UEPR** – Access granted to UEPR Servers, Local Workstation Administrator and AD Maintenance Delegate security groups
- **Service Delivery** – Access granted to Service Delivery Servers, Local Workstation Administrators Password Reset Delegate and AD Maintenance Delegate security groups.
- **Technical** – Access granted to Server Administrators, Local Workstation Administrators Password Reset Delegate and AD Maintenance Delegate security groups. Some Technical staff may require Domain Admin access to perform tasks.
- **Systems** – Access granted to Local Workstation Administrators Password Reset Delegate and AD Maintenance Delegate security groups. Some members of the Systems team may require access to the UEPR Servers group and some Systems staff may require Domain Admin access to perform tasks.
- **Projects** – Access to remain the same through Domain Admins. Access granted to Server Administrators, Local Workstation Administrators Password Reset Delegate and AD Maintenance Delegate security groups. Some Projects staff may require Domain Admin access to perform tasks.
- **Cyber Security** – Access granted to Server Administrators, Local Workstation Administrators Password Reset Delegate and AD Maintenance Delegate security groups. Some Cyber staff may require Domain Admin access to perform tasks.
6.0 REVIEW

6.1 On a monthly basis, a review of all elevated user accounts will be conducted with a view to determine if:

- The account has been used in the last 90 days (and disabled if not)
- If the account is still needed
- If the level of elevated privilege is still appropriate to the user.

7.0 REFERENCE OTHER DOCUMENTATION

7.1 The following documents should be read in conjunction with this Policy and its associated procedural guidelines:

- CP59 Data Protection and Confidentiality Policy
- CP74 Password Policy
- Admin Account Procedure