Mersey Care NHS
NHS Trust

TRUST-WIDE NON-CLINICAL DOCUMENT

Network Account Management Security Standard

Standard Number:	**SS06**
Scope of this Document:	**All Staff/ Services Users**
Recommending Committee:	**Joint Information Governance & Caldicott Committee**
Approving Committee:	**Joint Information Governance & Caldicott Committee**
Date Ratified:	**December 2015**
Next Review Date (by):	**December 2017**
Version Number:	**Version 1**
Lead Executive Director:	**Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian**
Lead Author(s):	**IM&T Security Manager**

TRUST-WIDE NON-CLINICAL DOCUMENT

2015 – Version 1

Quality, recovery and wellbeing at the heart of everything we do

Mersey Care NHS Trust

TRUST-WIDE NON-CLINICAL DOCUMENT

NETWORK ACCOUNT MANAGEMENT SECURITY STANDARD

Further information about this document:

Document name	**Network Account Management Security Standard SS06**
Document summary	**Trust Standard On the use of Internet and email**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 472 4031** **Mark.williams@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **Trust Headquarters** **V7 Building** **Kings Business Park** **Prescot** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IM&T Security Standard IT02**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Draft	Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian	December 2015

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Trust Standard and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

1 PURPOSE AND RATIONALE

1.1 **Purpose** –The purpose of this Standard is to prevent unauthorised access to the Trust's information systems and network services. The Standard describes how access control will be applied by the registration and de-registration process for all TRUST information systems and services.

1.2 This Standard forms a key component of Mersey Care NHS Trust's overall information security management framework and should be considered alongside the Trust's IM&T Security Policy IT02 and more detailed information security documentation including, system level security policies, security guidance and procedures.

1.3 This Standard is based on the principles identified within the NHS Code of Practice for Information Security and other related NHS policy and may be periodically updated as standards and guidance changes.

1.4 This Standard applies especially to new starters, leavers and those moving job responsibilities.

1.5 **Rationale** –In order to help maintain the security and integrity of the Trust electronic systems.

1.6 It is imperative that every system - whether accessed via local desktop PCs, communication networks and mobile devices, appropriate mechanisms for ensuring that only authorised users may gain access to information, programs, files and databases.

1.7 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.

1.8 Much of this control will be maintained by the use of user accounts and passwords.

1.9 The Trust recognises the value of information contained within their computer systems and will not tolerate unauthorised use. It is a criminal offence for an unauthorised person to attempt to access a system or information within systems or to attempt to exceed the computer facilities and privileges granted to them and the Trust will prosecute those committing any such offence as covered by the Computer Misuse Act 1990.

2 OUTCOMES AND OBJECTIVES

2.1 For this Security Standard the aims and objectives are as follows:

(a) To ensure that all staff are aware of their systems access control management.

(b) To ensure that staff use this standard guidance when requesting access to the Trust's Network, applications and clinical systems.

(c) To ensure Trust managers understand their responsabilities relating to employee starters, leavers and movers proccesses within the organisation.

(d) To highlight that failure to comply with the requirements of this Standard, can have serious impacts and consequences for the Trust.

3 SCOPE

3.1 This Standard applies to all employees of the Trust (or any person or persons providing a service to the Trust)

3.2 All Trust employees whilst engaged in work for the Trust at any location, on any computer or internet connection.

3.3 Any other use by Trust employees which identifies the person as a Trust employee or which could bring the Trust into disrepute on any computer or internet connection.

3.4 Other persons working for/with the Trust, persons engaged on Trust business or persons using Trust equipment and networks anyone granted access use of IT facilities over the Trust IT network.

4 RESPONSIBILITIES

4.1 Management are responsible for ensuring all staff within their department are aware of and understand the requirements of this Standard.

4.2 Managers are responsible for ensuring that the Service Desk and Systems Information Asset owners/administrators are notified when a member of staff leaves or moves so that access to systems can be terminated or adjusted.

4.3 Managers are responsible for the request for new accounts and to provide a definitive list of access requirements.

4.4 Information Asset Owners/Administrators must ensure that they act on information provided to ensure that user's access is granted/revoked when a user joins moves or leaves the Trust.

4.5 Information Asset Owners/Administrators must conduct regular audits to ensure user access is only granted to users on a need to know basis.

4.6 Users shall be mandated to keep all passwords confidential and in line with IG standards.

5 NEW STARTERS

5.1 Where a new starter is an employee of the Trust their information will be contained within the ESR feed. However, there is no guarantee that this users information is in ESR at the point of account creation so there are two possible scenarios as follows;

a) The Employees details are in the ESR feed

1) Locate the matching auto created account which will be present in the "_Auto Created Users" OU (use name, job title, NI as match criteria) – in all cases the data in the auto created account should be used as the authorities source.

2) Process the account as normal – group memberships/ passwords etc.

3) Move the AD account to the appropriate OU within the MCT OU.

b) The Employee details are not in the ESR feed

1) Create a new AD account for the user in the appropriate OU.

2) Process the account as normal – permissions/ passwords etc.

3) Enter the users NI into the AD account so it can be managed by the ESR feed.

5.2 Where a new starter is not directly employed by the Trust there will be no corresponding ESR feed data and therefore the AD account should be created from new as follows;

a) Non-Trust Employee (Contractor/ Temp etc.)

1) Create a new AD account for the user in the appropriate OU within the "MCT \ Non Trust Accounts" OU.

2) Process the account as normal – permissions/ passwords etc.

3) Enter the users NI into the AD account if known so it can be managed by the ESR feed if the user becomes an employee.

6 LEAVERS PROCESS

6.1 Staff leaving the Trust will have their IT account de-provisioned in one of the following ways

a) Automated de-provision. Where the leaver has an AD account that is managed by the ESR feed (i.e. has a matched NI) the account will be moved to the "_Auto Leavers" OU automatically on the day they leave the payroll system.

b) By Service Desk contact. Where the leaver has been identified by a line manager contacting the Service Desk, the Service Desk agent must disable the account and manually move it to the "_Auto Leavers" OU

c) Periodic manual audit/ clean-up Each month the Technical Services department will perform a manual audit of AD and move any non-employee accounts that have not been used within the last 30 days to the _"Auto Leavers" OU.

6.2 In each case, once the account has been moved to the "_Auto Leavers" OU the following actions will be processed on all accounts contained within via a daily scheduled task (commencing at 18:00)

a) The account will be disabled.

b) The description field will be updated with the date the account was disabled.

c) The email alias will be hidden from the Exchange address book.

6.3 Accounts will remain in this state for a period of two months, which is in line with current Trust policy, after which they will be deleted – along with all associated mailbox, home and roaming profile data. The Technical Services department will perform this function within the monthly audit cycle.

6.4 During their working life staff can take extended leave for a variety of reasons, depending on the type of leave, and if the staff member is an employee or not, the following process will be followed;

a) Maternity Leave

1) Employee: The user's details will remain on ESR and therefore no action is required, however if the user has made Service Desk contact to advise of this and does not want to receive emails while away they will be processed as non-employee below.

2) Non-Employee: The users account must be moved to the "_Extended Leave" OU, disabled, hidden from the address book and the account description changed to state: Maternity Leave

a) Long Term Sick Leave

1) Employee: As in the case of maternity, the user's details will remain on ESR and therefore no action is required. However if the user (or users line manager) does not want email's to be received by the account process as non-employee below.

2) Non-Employee: The users account must be moved to the "_Extended Leave" OU, disabled, hidden from the address book and the account description changed to state: Extended Sick Leave: 02/03/11 (where date is the day processed and in American format)

b) Career Break.

1) Employee: The user's details will be removed from the payroll at the point when they embark on the career break and therefore if we have not been informed by the user/ user's manager the account will be treated as a leaver and processed as such.

c) Where contact has been made process as follows;

1) The users account must be moved to the "_Extended Leave" OU, disabled, hidden from the address book and the account description changed to state: Career Break: 02/03/11 (where date is the day processed and in American format)

6.5 When the user returns to work they should make contact with the IT Service Desk to request their account be revived, this request should follow the normal process.

6.6 On occasion there will be a requirement for a colleague or line manager to access resources associated with a leaver, access to such resources will be granted as follows;

a) Access to Mailboxes

1) Where another user requires access to a leaver's mailbox the request will be granted for period of up to two months (the time the leavers account will remain on the system until it is deleted).

2) Access will be provided by allowing the user who needs access "Full Mailbox Access" rights to the leaver's mailbox and reconfiguring the mail profile.

6.7 Where another user requires the above for longer than two months the request and the reason for such request must be logged with the Service Desk and an appropriate will be provided.

a) Access to Home Drive

1) Where another user requires access to a leaver's home drive the contents of the leaver's home drive should be copied into home drive of the user requesting the access. However, consideration should be given to the size of the leaver's home drive before performing this operation – where the home drive equates to multiple GB guidance from senior technical support must be sought.

7 STAFF MOVEMENT

7.1 Where staff move or change roles within Mersey Care their current ***line manager is ultimately responsible*** for informing Informatics Merseyside and System Information Asset Owners/Administrators, of permissions that are no longer required. This needs to be completed via a Service Desk request.

7.2 Where staff move or change roles within Mersey Care their new ***line manager is ultimately responsible*** for informing Informatics Merseyside and System Information Asset Owners/Administrators, of permissions that need to be provided. This needs to be completed via a Service Desk request.

8 MAILBOX AND HOME DRIVE ACCESS

8.1 If access to another user's mailbox is required other than a leaver's mailbox, approval must be sought from the Service Director.

8.2 Access will be granted once approved to provide the least privileges required to carry out the tasks required.

8.3 If access to another users home drive or storage location other than a leaver, approval must be sought from the service director.

8.4 Access will be granted once approved to provide the least privileges required to carry out the tasks required.

9 PASSWORD MANAGEMENT

9.1 Passwords are confidential information and must be treated as such.
A password is only as secure as the person who knows it and as such the following standards must be adhered to:

a) Keep your system passwords safe.

b) Do not disclose them to anyone.

c) You will be forced to change your passwords from time to time for security purposes and inline with NHS guidelines.

d) Network passwords must be a minimum of 8 characters and contain at least 1 special character, one uppercase character and one number.

e) Should be easy to remember but difficult to guess.

f) Should not relate to information that is known to other members of staff.

g) Each user is responsible for maintaining the security of their individual login and password.

h) Staff must not share their user name or password with anyone.

i) Must not be written down unless kept in a sealed envelope and locked in a drawer.

9.2 Each user is responsible for maintaining the security of their individual login and password. If a breach of security is recorded under your login the burden of proof will be on you to show that you are not responsible for the breach.

9.3 passwords should be changed at regular intervals when requested by the system. This should be no less than 42 days.

9.4 If a password is forgotten the following steps must be taken;

a) Use the self service password reset function if available.

b) The member of staff must get their line manager to email the IT service desk requesting a password change. Alternatively the line manager can use the Service desk web form.

c) The IT service desk will then email the line manager with a new password.

d) The line manager must convey the password to the member of staff in person.

9.5 This Standard only covers passwords that are used for access to systems that have been installed and are maintained by Informatics Merseyside. Any passwords used for clinical or other computer based systems will be the responsibility of the 3rd parties, Information Asset Owners/Administrators supporting these systems and must be inline with HSCIC requirements.