North East Ambulance Service NHS

NHS Foundation Trust

North East Ambulance Service neasus Unified Solutions

Domain Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-5
Version Number	V04
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	18 July 2018
Date Policy Effective From	18 July 2018
Next Review Date	18 July 2021
Keywords	Access control; Account; Business critical information; Encryption; Mobile device; Network; Personal data; Removable media devices; Virtual Private Network (VPN)

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
1	All	First Draft	IG Manager	01 April 2012
2	All	• Updated in line with DNV recommendations and sections re-ordered with new monitoring table. • 3.2 Policy applies to all domain users (Trust staff and 3rd party users e.g. NDUC, Physiotherapists). • 4.3 Assistant Director of IM&T authorises access individual's file store or domain account. • 5.2.5 Group passwords must not be used for domain admin accounts. 5.6 - 9 Domain accounts are created by IM&T Service desk on receipt of ESR notification and permissions are based on job role. Contractor accounts will be based on NEAS equivalents or a new permission set determined by NEAS Sponsor.	IG Manager	April 2014
3	All	Reformatted into new template	IG Manager	Sept 2016
4	All	Full policy review	IG Manager	June 2018
		Following comments from consultation:	IG Manager	July 2018
	6.6	Shared Passwords replaced with Shared Accounts.		
	6.12 & 6.13 & 6.14	"Access for investigation purposes – with consent" AND "Access for investigation purposes – without consent" AND "Access for investigation purposes – external lawful authorities" combined and renamed "6.12 Access to an account for investigation purposes" Additional paragraph clarifies consent requirements.		
	6.13	This section is now "Access to an account for business continuity purposes" and clarification on consent.		
	6.14	Section on "Domain Equipment" removed as duplicated in 6.4.		
	6.17	HSCN replaced N3.		
	6.18	New section on Deactivation of Account.		

Table of Contents

1. Introduction

A Trust domain account is the means by which a registered user may carry out business using computers connected to the Trust domain. This account is the only official means of conducting Trust business electronically. Access is made to the account by the account-holder using the domain username provided by the IM&T Service Desk and Systems Team and the password associated with that username.

Each user must abide by all relevant external and internal regulations and there must be clear divisions of responsibility and privileges, with the legitimate corporate business of the Trust.

2. Purpose

The purpose of this document is to establish a standard for the administration and access of computing accounts within the Trust. The Trust must clarify how any domain computer account should be used and managed by the account-holder, whether he/she be a directly employed member of staff, contractor, temporary user or guest.

3. Scope

This policy covers both the Trust (North East Ambulance Service NHS Foundation Trust) and its subsidiary company North East Ambulance Service Unified Solutions (NEASUS). References to NEAS or Trust within this policy also cover NEASUS and its employees.

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, volunteer or contractor who holds a Trust domain account.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information security and risk management processes are providing them with adequate and appropriate assurances relating to risks against the Trust’s objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

4.4 Assistant Director of IM&T

Has responsibility for:

- Authorisation of requests for access to data to an individual's file store or domain account.
- Ensure Service Desk and Systems Team is aware of their responsibilities in line with this policy.
- Ensure effective management and authorisation of privileged accounts that IT administrator activities are logged and those logs are only accessible to appropriate personnel.
- Delegate admin account management to the IT Systems Manager where appropriate.
- Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.

4.5 Information Governance Manager

Has responsibility for:

- Developing, maintaining and implementing this policy.
- Undertake audit of access to the network and act on the results of these audits.
- Provide support and advise in implementing this policy to the Assistant Director of IM&T.

4.6 The IM&T Service Desk and Systems Team have a responsibility for:

- Process requests for domain accounts in line with their SLA (Service Level Agreement).
- Maintain an up to date user list within Active Directory in liaison with HR.
- Facilitate access control to domain accounts.
- Ensure the security of the domain, any Trust issued equipment and implement backup procedure.

4.7 All staff

All users are personally responsible for ensuring that they are aware of and compliant with this policy. By signing up to a Domain Account, users will agree to this policy and its guidelines and should be aware that a breach of this policy may be regarded as serious misconduct which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. Glossary of Terms

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Access control	Ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive.
Active Directory	An advanced, hierarchical directory service that comes with Windows servers and used for managing permissions and user access to domain resources.
Business Continuity	The preparation and testing of measures that protect business operations and also provide the means for the recovery of technologies in the event of any loss, damage or failure of facilities.
Disaster Recovery	The recovery of data stored on domain.
Domain	A group of computers and devices on a network.
File store	An area on the domain where information can be stored.
HSCN	Health and Social Care Network - data network for health and care organisations which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently.
IM&T Service Desk and Systems Team	A department within the Trust that responds to user's technical faults and service requests.
Sponsor	The person in the organisation who is responsible for authorising contractor domain accounts.

6. Policy Content

6.1 Domain Account

Trust staff, volunteers or contractors will generally be issued with a domain account for the duration of a contract of employment (or equivalent). The IM&T Service Desk and Systems Team will create a domain account on receipt of an ESR notification and completed ‘Request a Domain Account’ form. Access privileges will be assigned based on the user’s job role. If a user requires access outside their predefined access privileges, e.g. the user is on alternative duties for a temporary period, the line manager must notify HR so that changes to the job role may be made to IM&T systems.

The Trust manager responsible for any **contractor/volunteer** will need to advise HR of an account creation in ESR. The access privileges to be assigned to the user will be either the equivalent Trust job role or a new permission set based on the user need as determined by the Trust manager. They will also need to inform the IM&T Service Desk and Systems Team of any change to the status of the account, or to the agreed period of access.

6.2 Temporary / guest accounts

Temporary / guest accounts (auditors, interviewees, work experience) are designed to be temporary in nature (less than 5 consecutive days). The accounts do not have home directories or email accounts associated with them.

The user's sponsor within the Trust will request a temporary domain account through the IM&T Service Desk and Systems Team and will need to advise them of the access privileges to be assigned to the user.

It is the responsibility of the sponsor to inform the IM&T Service Desk and Systems Team of any change to the status of the account, or to the agreed period of access.

6.3 Admin accounts

Certain users will require additional access privileges to carry out their job role and they will be provided with an admin account to perform these duties. The IM&T Service Desk and Systems Team will create the username associated with the account in its standard structural format; generate a password of an adequate level of complexity and security, and will issue this password to the account-holder as the account's secondary access key. This password must not be divulged to any other person, other than by express, explicit and documented permission of the Assistant Director of IM&T and the continuing security of access is the responsibility of the account-holder.

A contractual agreement will need to be in place to grant third parties access to the Trust domain to perform administration on behalf of the organisation. This should be done through the **Guidance for Contracting a Data Processor Procedure**.

6.4 Access to a domain account

An account-holder's primary mode of access to the domain will be via a workstation which is connected to the Trust domain, either in a public-domain work area or in an office or similar environment. In this manner, the traffic transacted between the account-holder and the Trust domain lies wholly within Trust. Access may be made to a domain account from another location if the Trust is satisfied that an appropriate level of security is provided in making and using the connection.

The Assistant Director of IM&T has the discretion to allow or disallow access from any location or any mode and to change such designation at any time, for any purpose related to the free flow of primary-purpose Trust business or to the integrity of Trust data or computing services.

Accessing or attempting to access any part of the Trust domain including national and local applications, using any method other than your authorised personal username and/or password/smartcard/pin without the appropriate authority will constitute a breach of this policy.

It is not permitted at any time to use another user's personal username and/or password/smartcard/pin to gain access to any part of the Trust's domain. The person whose log on credentials are used will be held accountable for all actions during that login period to the domain. Breaching this policy may result in disciplinary action for both parties.

Access to a domain account by a person other than the account-holder may only be made with the express sanction of the Assistant Director of IM&T or their nominated representative. It is the responsibility of the accessor to ensure that all aspects of this policy and of any other relevant legislation and regulations are observed in any access to Trust data, and of the owner of the data to ensure that each permitted accessor is aware of the responsibilities associated with the granting of access and with the possibility of access restriction.

6.5 Passwords

Everyone granted authorised access to the Trust domain is issued a personal password, which forms part of his or her personal access credentials. Additional personal access credentials may be issued for access to national or local systems such as ESR (Electronic Staff Records) or Cleric.

If the security of the password is known or suspected to be compromised (actually or potentially), it is the duty of the user to inform the IM&T Service Desk and Systems Team immediately. The IM&T Service Desk and Systems Team on learning of any such actual, suspected or potential compromise from any reputable source, may (without the necessity of prior notification of the account-holder) revoke the password associated with any account, substitute another password of an adequate level of complexity and security, and may take any further steps deemed necessary to maintain the integrity of Trust data.

6.6 Shared accounts

Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares).

Shared accounts should only be considered where:

- Where access to a shared resource cannot be achieved in any other way.
- Where all participants must first log on to the domain/PC/laptop using their own personal access credentials before using a group password or
- In the case of training, where participants use a shared login and password to access a training PC but must then use their personal access credentials for further additional access.

Each shared account must have a designated owner who is responsible for:

- The management of access to that account.
- Formally documenting the requirement for a shared password.
- Maintaining an up to date list of all staff issued with access.
- Advising each participant of the other password holders.

- Changing the password when a participant leaves or no longer requires access.

Everyone using a shared account is responsible for ensuring it is kept confidential and solely within the members of the group. Group passwords must NOT be used to grant access to:

- Files or folders which are not part of the documented requirement.
- Any corporate or clinical information system.
- Network shares.
- Domain admin accounts.

6.7 File store

A domain account will give access to networked file store, some for the account-holder's own use (H drive), and some for managed shared use. If the account has a mail facility associated with it, a file store will be set aside for storage of mail and other messaging data. It is the account-holder's responsibility to manage all such file store effectively and practically, and to ensure that, in each case, data storage is compliant with all relevant legislation and policies i.e. Data Protection Act and Freedom of Information Act.

In addition to networked file store, the account-holder may have access to local file store held on a workstation's hard disk(s), and there may be the facility to write to removable media (floppy disk, CD, DVD, USB memory, etc.). As with networked file store, the responsibility to comply with all relevant legislation and policies remains with the account-holder. As standard, USB ports on all devices are disabled. Users requiring access should see advice from the IM&T Service Desk and Systems Team.

6.8 Records management

All data created and maintained within the Trust domain become the sole property of the Trust, unless there is an explicit agreement to the contrary agreed by the Chief Executive. The data, once created, edited or otherwise used, become subject to Trust records management policies and will, where relevant, become available for lawful disclosure to third parties (for example, under Freedom of Information legislation).

All users are responsible for regularly reviewing their own data storage areas removing unwanted files and freeing up storage space in conjunction with the Trust's document retention and disposal scheme (see the Records Management Policy.) This applies equally to users storing data on domain, local hard drive or removable media.

6.9 Personal use of the account

The Trust domain is provided to support users in their role for the benefit of our patients, staff and Trust. The use of the Trust domain for private purposes is not forbidden, but is subject to local management control and must be kept to a reasonable level, during break periods only, to avoid loss of productivity or distraction from primary tasks.

Whilst the data storage facilities within the Trust domain are specifically for business purposes, the Trust acknowledges that staff may store a small amount of private and personal data within storage areas on occasions. Whilst the Trust will take every reasonable precaution to safeguard staff privacy, this cannot be guaranteed, and staff are advised to remove any personal data promptly.

A domain account can be used for personal purposes as long as:

- It is not disproportionate to primary-purpose use, nor is in any way detrimental to the system's full availability for primary-purpose use.
- It is not for commercial, profit-seeking purpose, or for any financial gain to the sender or (by the agency of the sender's solicitation) to a third party.
- It does not conflict with the Trust's rules, regulations, policies and procedures.
- It does not conflict with the business of the Trust.

Data which are clearly labelled as personal, and which are stored accordingly and adequately separately from other data, will be observed as such in manual transactions, though automated data transactions will generally be unable to distinguish between the two types of designation.

6.10 Monitoring data

The Trust has a right to inspect, monitor or disclose data stored upon or passing through the Domain, but will not, as a matter of routine, do so unless:

- Required by law.
- For the purposes of maintaining the free flow of primary-purpose business.
- As part of an investigation of a suspected violation of the ordinances, rules, regulations or policies of the Trust.

Further information on monitoring of emails and the internet is found in the Email Usage Policy and Internet Policy.

6.11 Delegate access

Under certain conditions, full or partial access to data held in file store may be delegated by the account-holder to the holder of another account on the Trust domain. By such an action, the account-holder does not relinquish any responsibility with respect to the operation of the account. The agent also bears responsibility for compliance with all relevant policies, rules and legislation in carrying out any action on the delegator's account.

The delegation of any access is a serious matter, and must be carried out in accordance with the rules and policies drawn up by the Trust. All users should note particularly that it is forbidden to disclose any password which might allow another person to gain access in a manner which could lead to personation of the account-holder. The account-holder should maintain records which detail the timings and scope of any such delegation, whether a new delegation, a change to an existing delegation, or the withdrawal of delegate access.

It is important to realise that delegated access permission may not be controlled exclusively by technical means and the place of a verbal or written contract of instruction is not lessened by the existence (or otherwise) of technical controls.

Perhaps the most well-known instance of delegation within an account is the granting of full or partial access privileges to a PA or similar. In this instance, the delegate is acting as an agent for the principal.

There will be times when a principal will give delegate authority to a deputy during a period of the principal's absence. This will often be rolled in with other delegate powers (for example, to act and take certain decisions on behalf of the principal).

There are many instances within the Trust of data simultaneously made available to all members of a peer group. In the management of such data, the group members must always ensure that they act on behalf of the group. Each member of the group bears the responsibility to maintain group records, but the supervisor or other appointed head of the group bears ultimate responsibility for the management of all group records.

On occasion, there may be a need to grant access to a stand-in, possibly in an emergency. It is always helpful if the principal is able to make the delegation or consent to this, but with the agreement of the principal's line manager, the details of delegation may be conveyed to the IM&T Department if direct delegation is not possible.

Approval of the Assistant Director of IM&T will be necessary before any application made by a third party will be considered.

The scope of delegation should be clearly laid out in a message to the delegate, and this message should be retained and managed according to the standard procedures for task-related direction. This procedure is important in maintaining an ability to confirm the delegated powers in any dispute or investigation.

6.12 Access to an account for investigation purposes

During the course of a technical investigation into the domain service, there may occur the need for data to be processed in such a way that the content is disclosed within the investigative team. Each such investigation is different, but the following rules apply in each case:

- The use of accidental disclosure must be limited to the minimum level consistent with the investigative procedure.
- Any information gained by accidental disclosure is privileged information, and the use of such information must be limited to the investigative procedure.
- Further disclosure to any other person within the investigative team beyond the minimal scope necessary to the investigation is not permitted.

Any investigator who operates beyond the scope of the investigation with respect to accidental disclosure will be subject to the appropriate disciplinary procedures of the Trust.

Consent to access the account from the account holder is not normally required if it is believed that there is a potential breach in any Trust policy. However, anything clearly identified as falling within 6.9 or marked personal e.g. communications with Occupational Health or a recognised Trade Union may not be accessed. Each investigation must be on a case by case basis and additional advice can be sought from the IG Manager.

The Assistant Director of IM&T will co-operate with any investigation by external lawful authorities, granting such access as is backed up by the appropriate Production Order, warrant or similar document, within the provisions of the appropriate legislation. Any information gained by any member of an investigative team is privileged.

6.13 Access to an account for business continuity purposes

If the business continuity of the Trust is put at risk due to unforeseen absence of an account-holder, the line manager may request that delegate powers be assigned as if the account-holder has made such an assignment. The scope and duration of the delegation must be confirmed and the line manager will take responsibility for the good conduct of the delegate(s), and for the eventual management of the records created, edited or deleted on the delegated account. It is always advised that consent should be sought to grant access. However, if this is not possible, then additional advice can be sought from the IG Manager.

6.14 Training laptops

Where encrypted laptops and USB data storage devices would prevent external users from accessing facilities provided by the Trust, with the authority of the Assistant Director of IM&T, they may remain unencrypted, providing managers in Training ensure:

- IM&T services configure the laptops to deny accidental access to the Trust’s domain.
- Equipment is clearly marked “Unencrypted Device – do NOT connect to Domain or store any confidential data”.
- External users are made aware Training staff manually purge all training equipment of student data at the end of each course.
- All training equipment is properly managed and secured when not in use through physical access control (locked away) and technical access control (using passwords).

6.15 Meeting room / interview equipment

Meeting room equipment will allow access to the domain and section 6.2 should be consulted. If the user needs to connect their own device to projection equipment, they may do so but this will not grant them access to the domain. They may use their own equipment to access guest Wi-Fi and their Trust sponsor must request this through the IM&T Service Desk and Systems Team.

Encryption of Trust equipment will prevent external users from using their USB device. Arrangements should be made between the user and the Trust sponsor to access such information i.e. emailing the information. If there is a requirement to use an external USB device on Trust equipment, IT will create an exclusion for that particular device after it has been fully scanned for viruses. A Service Desk request must be made in advance.

6.16 Data backup

Backup files are kept under the control of the Trust for the sole purpose of disaster recovery and business continuity on a system-wide basis: they are not regarded as an ‘offline repository’ in any capacity, or as a backtracking facility for the restitution of individual files following a reconsideration of the wisdom of any editing or disposal.

The IM&T department will undertake and manage the backing up of all domain drives on a regular basis. Staff that do not have access to a domain drive for data storage are responsible for managing their own regular data back-up.

6.17 Equipment security

To preserve the security of Trust’s information asset:

Only Trust owned or formally contracted/leased hardware, software, media and related equipment may be used:

- Within any part of the Trust’s Computer System and
- To conduct the Trust’s business.

Hardware, software or media not owned/contracted/leased by the Trust, must never be installed or connected to any part of the Trust domain or used to conduct Trust business. This specifically prohibits:

- The installation or connection of any personally owned software, hardware or media by staff to the Trust domain.
- Use of any personally owned software, hardware or media to conduct the Trust’s business, regardless of location.

Non-compliance may create an immediate major security breach, jeopardise the Trust’s NHS domain (HSCN) connection and may result in disciplinary action.

6.18 Deactivation of account

The account will be disabled at the dissolution (through resignation, retirement or other reason for termination) of the contract of employment (or equivalent). There will be no right of access by the account-holder following this.

HR will normally notify IT via ESR that a member of staff is leaving and IT will disable the account which means it can no longer be accessed. The data stored in the account (e.g. email, documents) are not deleted as such. Leavers and their manager should begin preparations for this event in good time - at least one month in advance if possible. They should review what data is necessary to keep in line with the Records Management Policy.

It is the line manager’s responsibility to ensure any IT equipment assigned to the user is returned to the IT department including laptops, USB devices etc.

IT will also run monthly reports of stale accounts identifying those accounts which haven’t been used for 6 months. Any identified will be automatically disabled and moved to a holding area prior to deletion. Leaver’s accounts will be deleted after 12 months.

7. Training Required for Compliance with this Policy

All staff to receive Mandatory Information Governance Training on an annual basis.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	The number of active domain accounts against the ESR staff list. Evidence of consent being sought for access to another users' domain accounts. Number of domain account breach incidents.

When will the monitoring be performed?	Active domain accounts- Bi-annually. Consent through IG team. Breaches - Every other month.
How are you going to monitor?	Via Ulysses reports and IM&T Service Desk and Systems Team.
What will happen if any shortfalls are identified?	Logged in risk registers and/or Ulysses.
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	The action plan will be progress by the Information Security Working Group and monitored by the Information Governance Working Group.
How will learning take place	Learning will be via the action plans and monitored by Information Governance Working Group.

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with the Information Governance Working Group, Information Security Working Group, SIRO and Executive Directors.

11. Implementation of this Policy

This Policy is to be implemented Trust wide, through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- Data Protection Act
- Freedom of Information Act

13. Associated Documentation

This policy refers to the following Trust documents:

- Email Usage Policy POL-F-IMT-12
- Internet Policy POL-F-IMT-9
- Records Management Policy POL-F-IMT-10
- Guidance for Contracting a Data Processor