necs A care system support organisation

NHS

IT Access Control Policy

Author: Gary Ingham
Date: 26/02/2025

Information reader box	
Directorate	
Business information services	
Publications gateway reference	
Document purpose	**Policy**
Document name	**IT Access Control Policy**
Author	**Gary Ingham, ICT Compliance Manager**
Publication date	26/02/2025
Approving body	**NECS Executive Group**
Target audience	**All users including staff, contractors, consultants, temporary and other workers in NECS. Customers receiving IT services provided by NECS, and suppliers where their terms of business with NECS, require adherence to the NECS IT Access Control Policy.**
Additional circulation list	N/A
Description	**Policy**
Cross reference	N/A
Superseded document	**IT Access Control Policy v2.1**
Action required	**Compliance**
Timing/deadlines	N/A

Contact details (for further information)

Gary Ingham ICT Compliance Manager
Tel: 0191 374 2779
Email: garyingham@nhs.net

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.

Document information

Staff who become aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives that affect, or could potentially affect policy documents, should advise the sponsoring director as soon as possible, via line management arrangements. The sponsoring director will then consider the need to review the policy or procedure outside of the agreed timescale for revision

Accessible Information Standards
If you require this document in an alternative format, such as easy read, large text, braille or an alternative language please contact NECSU.comms@nhs.net

Contents

1. Policy statement

The purpose of this Policy is to define the key principles, parameters and requirements for the provisioning, management, and revocation of access to all NECS information assets and systems, to ensure that all information is suitably protected at all times and only those that require access have it. This will form the basis of the underlying fundamental rules on which procedures are developed.

All access control processes and procedures must be derived from this Policy and are to be followed at all times when provisioning user access to all NECS network, systems, applications, and databases, capable of storing or processing any NECS information assets.

This Policy is intended to reduce the risk of users acquiring inappropriate access to computer networks, by ensuring that only appropriate access privileges are granted to users, that access rights are amended in alignment with any changes to the user's role, that access is revoked in a timely manner upon the user ceasing to require access, and that sufficient security measures are implemented to provide effective information security.

2. Introduction

Information security is the protection of information against accidental or malicious disclosure, modification, or destruction. Information is an important, valuable asset which must be managed with care.

Access controls are put in place to protect information by controlling rights to different information resources and guarding against unauthorised use. In order to adequately protect and restrict access to information held within the network and associated systems, formal processes have been established to guide the provisioning of user access, information access, and network access.

Access to the network and associated systems provided by NECS (including hardware and software sources such as database servers, folders, and software applications) is primarily controlled using Microsoft's Active Directory (AD). Locally managed systems will have their own documented procedures covering access control, but where possible will follow the principles set out in this Policy.

3. Scope

The scope of this Policy applies to the networks and systems managed within NECS:

NECS corporate network (comprising of)

- Systems, applications, databases, hardware, and software
- Cloud solutions
- National NHS Solutions managed via NECS Registration Authority Procedure
- NECS customers
- NECS suppliers

3.1. Definitions

The following terms are used in this document:

Active Directory (AD) – Windows Active Directory System is a directory service used for domain and user management. For the purpose of this Policy 'AD account' is interchangeable with the term 'network account'.

Azure Active Directory (AAD) – is Microsoft's cloud-based identity and access management service for employees, customers, and suppliers i.e. MS Office 365, cloud-based SaaS applications.

Line Managers - are individuals that have been deemed to be in a position of sufficient responsibility and are granted the power of approving new standard account creations onto the network.

Generic Account - is a term used to describe any account that is shared by multiple users and where the use of the account cannot be easily attributed to an individual e.g. GP locum accounts.

Locally Managed systems - is the term used to describe those systems which do not have NECS IT support for user access management, such as user access administration and the changing of passwords, undertaken within the system e.g. ESR.

Information Asset Owner/Administrator (IAO/A) – are senior individuals e.g. Heads of Service/Senior Managers involved in running NECS/Customer business. Their role is to understand what information is held, what is added and what is removed, how information is moved and who has access and why. As a result they are able to understand and address risks to information and ensure that information is used appropriately and provide updates to the SIRO.

Local Privileged Account - an account that is considered to have heightened privileges that is restricted only to a local server and/or local machines. No access to the wider network

exists. This type of account is only granted, where business justification has been considered appropriate.

Highly Privileged Account (Administrator) - in the context of this Policy, NECS considers a 'privileged user' to be any user who possesses one or more of the following AD privileges:

- Built-in Administrator
- Domain Admin
- Server Operators

This type of user is able to make changes to settings and configurations that can affect the whole network.

Standard Network Account - is an initial Windows AD account which is allocated to staff, contractors and customers that receive an IT service from NECS. Standard users will have limited privileges on the network; if additional access is required, it will be allocated following appropriate authorisation.

Service Account - is an account which may possess heightened privileges that is used to run a service or routine without human intervention, and as such is not usually logged into by users.

Third Party Account - is an account created for the intended use by a non-NECS employee or customer. Third party accounts may have heightened privileges to allow provision of outsourced services and/or technical support.

Test Account - is an account created for the sole use of testing a service or functionality. Test accounts may have heightened privileges where high level testing is required.

4. Roles and responsibilities

4.1 Accountable Officer

The Accountable Officer has overall responsibility for ensuring that information is handled appropriately in order to protect information from unauthorised disclosure or misuse. This role is carried out by the Managing Director.

4.2 Director of Business Information Services

The Director of Business Information Services is the sponsoring director for this document and is responsible for ensuring that this Policy remains up to date and that all staff and managers adhere to the processes outlined within this Policy.

4.3 Information Asset Owners

The Information Asset Owner will:

- Be responsible for granting/removing access to any data and identified locally managed systems they are responsible for e.g. ESR

With regards to information stored on the Shared Drive/Teams

- Reject any inappropriate or suspicious authorisation requests
- Inform IT of any known leavers to enable any applicable accounts to be disabled
- Inform IT of any changes to folder owner (e.g. if they leave post).

4.4 Line Managers

Line Managers will:

- Be responsible for approving new user access
- Reject any inappropriate or suspicious authorisation requests
- Inform NECS IT Service Desk of any known leavers, to enable any applicable accounts to be disabled, or by raising a call via the IT Service Management system.
- Notify IT via the IT Service Management system of employees on maternity or long-term sick leave (classified as three-hundred days or more).

4.5 ICT Service Managers

ICT Service Managers will;

- Distribute relevant information within this Policy to any Third-Party suppliers, who have been provided with a Third-Party account on the NECS network.
- Be responsible for approving Microsoft AD and Azure AD (AAD) privileged access

4.7 Customers

Customers will:

- Adhere to all applicable elements of this Policy, any deviation from this may result in an incident being raised and access being revoked
- Reject any inappropriate or suspicious authorisation requests, where applicable authorisation rights exist
- Inform the ICT Service Desk of any known leavers to enable any applicable accounts to be disabled in a timely manner
- Only access information they are authorised to access for their intended purpose and duration
- Not copy, download, or retain any information without the explicit consent of NECS, prior to leaving the organisation.
- Report any experienced degradation in access to the ICT Service Desk.

4.8 Third Party Suppliers

Third Party Suppliers will:

- Adhere to all relevant information in this Policy, any deviation from this may result in an incident being raised with the ICT Service Desk and access being revoked
- Only use and access information intended for them to deliver their service
- Not copy, download, or retain any information without the explicit consent of NECS
- Not share any user credentials for anything they are granted access to
- Report any experienced degradation in access to the ICT Service Desk.

4.9 All staff

All staff (permanent, temporary, agency, contractors, secondees, supplier and customer staff) are responsible for:

- Compliance with this Policy and relevant processes. Failure to comply may result in disciplinary action being taken
- Co-operating with the implementation of this Policy as part of their normal duties and responsibilities
- Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional standards and local/national directives, and advising their line manager accordingly.

5. User Provisioning

5.1 Key Principles

NECS adopts the principle of least privilege. Heightened privileges must only be granted and used when absolutely necessary.

No access to systems or information assets is to be allocated without the appropriate authorisation, see 5.2 Granting Access. Only known individuals with a genuine business need should be granted access.

Generic accounts are permitted, when appropriately authorised.

All contractors, agency staff and third-party accounts must be allocated temporary accounts (which are end dated), due to the nature of their temporary employment.

Default administrator account passwords must be unique across the environment and changed on a regular basis, where used.

5.2 Granting Access

NECS User Access Management Procedures document the process to be followed upon granting different levels of access to the NECS network, ensuring appropriate authorisation has been provided and only required access is granted, necessary to complete the users job role. The document covers all stages of the lifecycle of users access, from initial creation, approval and removal when access is no longer required. Such procedures are also documented for any locally managed systems and are the responsibility of the IAO.

5.3 Amending Access

Any user identified as moving organisation, department or team are to have their access reviewed. Any access that is no longer appropriate is to be revoked in a timely manner.

Movers to or from NECS or customer organisations are the responsibility of their respective managers. Where the manager assesses that the access rights need to be amended or revoked, the relevant IAO of any locally managed systems the user has access to, and the ICT Service Desk in the case of network access, must be informed.

Any additional privileges must be approved before allocation.

5.4 Revoking Access

Accounts belonging to leavers will be disabled/removed upon positive confirmation that the individual has left the organisation and has not moved to any other organisation receiving IT services from NECS.

6. Data Access Management

6.1 Authorisation

Each folder stored on the Shared Drive must have a designated Folder Owner, responsible for authorising access to the folder.

Access to a folder will not be allocated unless a fully authorised folder access request is received.

Access to any data stored within channels on Microsoft Teams, will need approved by the channel owner. These requests go directly to the channel owner via email.

6.2 Amending / Revoking access

Line managers and Folder/Channel Owners are responsible for informing IT when staff members no longer require access to folders.

Upon notification, data access will be revoked.

7. Access Reviews

On a regular basis (specified frequencies are documented within procedures), information asset owners will review access to ensure:

- Only users who require access, have access
- The different levels of access available are appropriate for the user to fulfil their job role
- Any leavers and/or movers are identified and removed accordingly

Upon completion of a user access review, any follow up actions will be completed and recorded on relevant audit documentation, where required.

8. User Authentication/Password Management

A strong password is an essential barrier against unauthorised access.

All passwords must adhere to NECS standard as confirmed in NECS IG Fact Sheet 14 – Information Security at Work and in the Home. Where a system cannot comply due to system restrictions, the configurations will be set to the strictest security settings available, in order to provide sufficient information security protection, unless justification exists for reduced security.

All default passwords must be changed in accordance with the NECS IG Fact Sheet 14 – Information Security at Work and in the Home.

It is understood that passwords alone may not protect data, and thus there are numerous other ways to improve the security of user authentication, including various forms of two factor authentication methods.

Multi-Factor Authentication (MFA) should be enabled on all systems that contain NECS data, in line with NHSE MFA Policy.

NECS will provide staff with access to MFA methods as appropriate, to enable them to access the systems needed to perform their role, as covered in the NECS Acceptable Use Policy. Current methods include smartphone apps and text messages (SMS). Other methods may be introduced as appropriate technology develops and matures and may require the use of NECS or non-NECS issued devices by staff or partners.

9. Incident Reporting

Incidents must be reported in accordance with the NECS Incident Reporting and Management Policy Implementation and Distribution.

10. Distribution and implementation

This Policy will be available to all staff for use in relation to access control management, via the NECS Intranet and NECS Internet https://www.necsu.nhs.uk/who-we-are/our-policies/

All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood this document and are competent to carry out their duties in accordance with this Policy.

It will be the responsibility of the Information Governance Committee to support the implementation of this Policy across NECS.

All staff will be notified of a new or revised document via a Team Talk bulletin.

11. Monitoring

The monitoring of this Policy will be ensured by the Information Governance Committee Work Programme.

12. Impact analysis

As part of the development of this policy, its impact on equality has been assessed and no issues identified.

The Equality Impact Assessment Screening Assessment can be found at Appendix 1.

13. Associated documentation

13.1. Other related policy documents

This Policy is written in conjunction with the following policy documents:

- NECS IT Acceptable Use Policy
- NECS Incident Reporting and Management Policy
- NHS England Information Governance Policy
- NHS England Information Security Policy
- NHS England Corporate Documents & Records Management Policy
- NECS Registration Authority Procedure

Further details of other documents are outlined in the following procedural documents:

- User access management procedures/sops
- NECS IG Fact Sheet 14 – Information Security at Work and in the Home

13.2. Legislation and statutory requirements

This Policy is written in adherence with the following requirements:

- NHSE Data Security and Protection Toolkit
- ISO27001 Standard

14. References

None.

Appendix 1 - Equality impact assessment

Initial screening assessment (Step 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Gary Ingham

Job Title: ICT Compliance Manager

Organisation: NECS

Title of the service/project or policy: : IT Access Control Policy

Is this a;

Strategy / Policy ☒ Service Review ☐ Project ☐

Other Click here to enter text.

What are the aim(s) and objectives of the service, project or policy:

The purpose of this Policy is to define the key principles, parameters and requirements for the provisioning and revocation of access to the AD network, information assets and systems to ensure that all information is suitably protected.

Who will the project/service /policy / decision impact?

(Consider the actual and potential impact)

- **Staff** ☒
- **Service User / Patients** ☐
- **Other Public Sector Organisations**☐
- **Voluntary / Community groups / Trade Unions** ☐
- **Others, please specify** Customers/Third party suppliers

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	☐	☒
Has there been or likely to be any staff/patient/public concerns?	☐	☒
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	☐	☒
Could this piece of work affect the workforce or employment practices?	☐	☒
Does the piece of work involve or have a negative impact on: • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community	☐	☒

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed

policy/project/service change, please state how you have reached that conclusion below:

The review of the questions above show that there is no impact. The Policy applies equally to all staff, customer and supplier groups as stated in this Policy.

If you have answered yes to any of the above, please now complete the

'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	☒	☐
If any of the above have not been implemented, please state the reason: N/A		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	**Job title**	**Date**
Gary Ingham	ICT Compliance Manager	14/01/2025

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

If you are not completing 'STEP 2 - Equality Impact Assessment' this screening document will need to be approved and published alongside your documentation.

Please send a copy of this screening documentation to:
NECSU.Equality@nhs.net for audit purposes.

Appendix 2 - Version Control Tracker

Guidance on version control is set out in Appendix B of NECS Information labelling and Classification Procedure

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
2.1	04/07/2024	Gary Ingham	Final	Amendments made during review: • Updating of document data classification to Official. • Update of ICT Compliance Manager to Gary Ingham. • Section 5.4 Revoking Access – addition of the disablement script being run every 30 days, to capture any newly created user accounts that are not logged into. • Entire document updated to indicate the frequency of audits • Section 7.1 Standard Network Accounts updated to include an audit of standard user accounts. • Section 7.3 Highly Privileged Accounts updated to include privileged account creation check. • Addition of Version Control Tracker to document Minor changes approved at IGC 04/07/2024
3.0	26/02/2025	Gary Ingham	Final	Full document reviewed to remove specific procedural information and ensure the document only details the access control principles. Update to document owner Approved at IGC 21/01/2025

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
				Approved at Formal Exec 26/02/2025