A care system support organisation

IT Access Control Policy

Information Reader Box

Directorate	
Business Information Services	
Publications Gateway Reference	
Document Purpose	Policy
Document Name	IT Access Control Policy
Author	Alison Emslie, ICT Compliance Manager
Publication Date	26/11/2021
Approving Body	NECS Executive Group
Target Audience	All users including staff, contractors, consultants, temporary and other workers in NECS, receiving IT services, provided by NECS, customers and suppliers, where their terms of business with NECS, require adherence to the NECS IT Access Control Policy and in so far, as the services they receive from NECS, are relevant to the policy.
Additional Circulation List	N/a
Description	Policy
Cross Reference	N/a
Superseded Document	IT Access Control Policy v1.4
Action Required	Compliance
Timing/Deadlines	N/a

Contact Details (for further information)

Alison Emslie, ICT Compliance Manager
Tel: 0191 217 2878
Email: alison.emslie@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**

If you require this document in an alternative format such as easy read, large text, braille, or an alternative language please contact Alison Emslie, ICT Compliance Manager

1 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).

AD security controls are configured to enable access to the NECS network and NECS information assets. AD allows passwords to be configured and disseminated across the whole NECS Infrastructure.

Access to information assets are controlled through folder management within AD. Access is restricted to appropriate individuals and granted through dedicated Information Asset Owners.

3 Scope

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

NECS Corporate Network (comprising of)

- Systems, applications, databases, hardware, and software
- Cloud solutions
- NHS wide (National NHS Solutions) managed via NECS Registration Authority Procedures
- 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.

Folder Owners - are individuals that have been deemed to be in a position of sufficient responsibility and are granted the ownership of controlling access to a specified folder.

Guest Account - is a default account with associated default passwords, intended for the use by "guests" of 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 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 is - 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.

Organisational Unit (OU) - is an AD container into which users, groups, computers, and other organisational units can be placed, enabling a set of permissions or rules to be applied to that group.

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 identified locally managed systems they are responsible for e.g. ESR

4.4 Line Managers

Line Managers will:

- Be responsible for approving new user access to the network
- 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

4.6 Folder Owners

Folder Owners will:

- Be responsible for approving new user access to the folder of which they have ownership
- 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).

4.7 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 Manager 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. Standard network accounts will not be granted domain administrator privileges. Users requiring heightened privileges must be allocated an additional account for carrying out administrative roles.

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.

All account passwords must conform to the specifications outlined within the NECS IG Fact Sheet 14 – Information Security at Work and in the Home.

No account belonging to an individual user is permitted to have a non-expiring password. Service accounts are permitted to have non-expiring passwords.

No access to servers will be granted through a standard user account, access must only to be granted through using Highly Privileged account.

All accounts that are interactively logged onto must have a clearly defined owner. Service accounts must clearly be identifiable as a service account and must contain information describing their purpose.

Generic accounts are permitted, when authorised by ICT Compliance or IT Security and supported by a genuine business need (a small number of third party, IT accounts and GP practice accounts).

All contractors, agency staff and third party accounts must be allocated temporary accounts due to the nature of their temporary employment. All temporary accounts (including third party and test accounts) must be 'end dated' as outlined on the relevant form and/or change request. If no date is specified, network access cannot be granted.

All test accounts that are created must be clearly associated to an individual; this must be reflected in the account name or clearly stated in the account description. Once testing has been completed test accounts must be deleted. This is the responsibility of the owner of the test account.

All guest accounts are disabled and not permitted for use, on NECS devices.

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

5.2 Granting Access

All network accounts created (with the exception of test accounts with standard user privileges) must be authorised by a line manager prior to account creation.

Authorising individuals must be an individual in a position of seniority over any individuals that they are authorising to have access.

Privileged access (AD/AAD) (including service accounts) may only be granted following appropriate authorisation. This authorisation must be provided in addition to authorisation for standard accounts or if the required access is additional to any existing access. Every individual request must be accompanied by an individual associated authorised form.

Local privileged accounts (including local server access) may be authorised by the Infrastructure Systems Manager and IT Security. This must be requested via a Service Account request within the IT Service Management System.

Temporary Third party access may only be granted following agreement of NECS Terms and Conditions and appropriate authorisation as outlined on the Third Party Request form. A further request is to be made for the re-enablement of the account.

If a test account does not require heightened privileges or access then it may be created without any authorisation at the discretion of the IT engineer carrying out the testing.

No access (including privileged access) must be allocated to any account other than that clearly stated on the associated authorisation form.

5.3 Amending Access

Any users 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 respective managers. Managers must inform NECS IT by raising a leavers request in the IT Service Management System, to allow any amendments to be made to the privileges of their staff.

Any additional privileges must be approved before allocation.

5.4 Revoking Access

AD User accounts that are inactive for over 60 days will be automatically disabled.

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

Accounts and all associated information are eligible for deletion following a 12 month period of being disabled. It is the responsibility of the individual employee and their Line Manager to ensure that all information is transferred onto a shared network drive or folder, prior to the employee leaving the organisation.

5.5 Maternity/absence

Upon IT receiving notification of long-term absence or maternity leave, accounts are temporarily disabled and protected from deletion.

It is permissible for users on maternity and long-term absence to access their account during the absence if required. However, the respective line manager, must request the account to be re-enabled (if disabled).

5.6 Re-enabling Disabled & Expired accounts

Line Manager approval must be given prior to an account being re-enabled.

For an expiry date to be extended, an Account Re-enable/Extension request must be made via the IT Service Management Customer Portal.

6 Folder Access Management

6.1 Authorisation

Each folder 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.

6.2 Amending / Revoking access

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

Upon notification, folder access will be revoked.

7 Access Reviews

7.1 Standard Network Accounts

Regular access reviews of standard user accounts take place by ICT Compliance Team.

Accounts found to have inappropriate access will have their access amended as required.

In the event that a significant number of accounts have inappropriate access an incident shall be raised, and investigation commenced.

7.2 Third Party Accounts

ICT Compliance team undertake regular reviews of all Third Party account requests, to ensure their access has been created as requested.

7.3 Highly Privileged Accounts

A regular review of privileged accounts appropriateness and non-expiring passwords, (including service accounts) is the responsibility of IT Security and is to be completed in collaboration with IT Infrastructure Systems.

Any access found to be inappropriate must be amended in a timely manner.

7.4 Folder Access

Folder access will be reviewed once per year, by the ICT Compliance Team.

Any users found to have inappropriate access shall have their access revoked in a timely manner.

Any inappropriate authorisers or Folder Owners must have their privileges revoked.

7.5 SQL Privileged Accounts

The Head of Data and Digital Applications will ensure regular reviews of all SQL privileged accounts are conducted.

7.6 System Access

Reviews of access on systems or applications must be carried out in accordance with System Level Security Procedures and are the responsibility of the system or application owner (IAO/IAA).

8 Password Management

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.

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 the procedures described.

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 an Essentials bulletin.

11 Monitoring

The Director of Business Information Services, as sponsor director, will agree with the ICT Compliance Manager a method for monitoring the dissemination and implementation of this Policy. Monitoring information will be recorded in the policy database.

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

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

- NECS IT Access Control Procedures
- Records Management Code of Practice for Health and Social Care 2021
- 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:

- NHS Digital 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: Alison Emslie
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** Click here to enter text.

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**
Alison Emslie	ICT Compliance Manager	09/01/2023

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.