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 Tel: 0191 217 2878 Email: alison.emslie@nhs.net
Publication Date	26/11/2021
Approving Body	NECS Executive Group
Target Audience	All IT 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Superseded Document	IT Access Control Policy v1.3
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.

Contents

1. Introduction 5
1.2 Status 5
1.3 Purpose and scope 5
1.3.2 Scope 6
2. Definitions 6
3. Duties and Responsibilities 9
3.1 Accountable Officer 9
3.2 Director of Business Information Services 9
3.3 Access Control Team 9
3.4 Head of Data and Digital Applications 10
3.5 Human Resources Team 10
3.6 Approved Authorisers 10
3.7 ICT Service Managers 10
3.8 Folder Owners 11
3.9 Customers 11
3.10 Suppliers 12
3.11 All staff 12
4. User Provisioning 13
4.1 Key Principles 13
4.2 Granting Access 14
4.3 Amending Access 15
4.4 Revoking Access 15
4.5 Maternity / absence 15
4.6 Re-enabling Disabled & Expired accounts 15
5. Folder Access Management 16
5.1 Authorisation 16
5.2 Amending/ Revoking access 16
5.3 Information Classification 16
6. Access Reviews 16
6.1 Standard Network Accounts 16
6.2 Privileged Network Accounts 17
6.3 Folder Access 17
6.4 Authorisers 17

6.5 SQL access....17
6.6 System Access....17
7. Password Management....18
8. Physical Access....18
9. Incident Reporting....18
10. Implementation and Distribution....18
11. Training Implications....19
12. Monitoring, Review and Archiving....19
12.1 Monitoring....19
12.2 Review....19
12.3 Archiving....20
13. Documentation....20
13.1 Other related policy documents....20
13.2 Legislation and statutory requirements....20
14. Appendix A....21

IT Access Control Policy

1. Introduction

1.1 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 security framework solution Active Directory (AD) and/or Microsoft Azure AD (AAD). The AD and AAD security controls configure and enable access to the NECS network and NECS information assets AD/AAD allows passwords to be configured and disseminated across the whole NECS Infrastructure; mandated configurations are outlined within this policy.

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

1.2 Status

This policy is an IT policy.

1.3 Purpose and scope

1.3.1 Purpose

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.

1.3.2 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 Policy and Procedures
    - NECS Customers
    - NECS Suppliers

2. 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 which help you configure and manage access for employees, customers and suppliers i.e. MS Office 365, cloud based SaaS applications.

Approved Authorisers are individuals that have been deemed to be in a position of sufficient responsibility and accountability by IT Security and are granted the power of approving new standard account creation onto the network.

Disabled Account is an account that has been flagged as disabled within AD, preventing the account from being logged onto.

Expired Account is an account with a date that has exceeded the permissible date enforced on the account, preventing the account from being logged onto. The account will be automatically locked out once the specified end date has been exceeded.

Folder Owners are individuals that have been deemed to be in a position of sufficient responsibility and accountability by Access Control, 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 guest users 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.

IT Supported Systems is the term used to describe those systems supported by the NECS IT Teams which include user access management such as user access administration and the changing of the local system passwords e.g. AD.

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. Oracle.

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.

National Support Systems is the term used to describe those systems supported at a national level such as EMIS, SystmOne.

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.

Privileged Network 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, Enterprise Admin, Domain Admin, Schema Operators, Backup Operators, Account Operators, 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.

SQL Privileged Account, NECS considers an 'SQL Privileged user' to be any user who possesses the 'SysAdmin' Database Privilege. This type of user is able to make changes that affect database configurations and data.

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.

Temporary Account is an account for temporary use only.

3. Duties and Responsibilities

3.1 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.

3.2 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.

3.3 Access Control Team

The Access Control Team will:

- Be responsible for producing, maintaining and circulating Administrator Access and Third Party Access Forms.
- Conduct quarterly reviews of all Privileged Accounts.
- Conduct sample based user access reviews of standard user accounts.
- Be responsible for updating this Policy.

- Ensure that all Access Control. Staff receive training to ensure that they understand and adhere to the processes outlined within this Policy.
- Conduct monthly internal checks to confirm processes are being followed correctly

- Be responsible for the management and maintenance of the Online Access Portal.

3.4 Head of Data and Digital Applications

The Head of Data and Digital Applications will ensure:

- Regular reviews of all SQL privileged accounts are conducted.

3.5 Human Resources Team

The HR team will:

- Be responsible for removing access to any identified systems HR manage.
- Be responsible for sending a notification to the relevant ICT departments for NECS leavers
- Be responsible for notifying NECS and CCG (for which NECS provides HR support) employees on maternity or long term sick (classified as three-hundred days or more) to IT on a monthly basis.

3.6 Approved Authorisers

Approved Authorisers will:

- Be responsible for approving new user access to the network.
- Reject any inappropriate or suspicious authorisation requests
- Inform IT of any known leavers to enable any applicable accounts to be disabled

3.7 ICT Service Managers

Service Managers will;

- Act as the account managers or liaise with the account managers in relation to supplier's adherence to this Policy

3.8 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)

3.9 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 relevant ICT departments 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 to copy, download or retain any information without the explicit consent of NECS
- Should any degradation in access be experienced this will be logged with the relevant ICT ServiceDesk.

3.10 Suppliers

Suppliers will:

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

3.11 All staff

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

- Compliance with relevant process documents. Failure to comply may result in disciplinary action being taken.
- Co-operating with the development and implementation of policies and procedures and 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.
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training / awareness sessions when provided.

4. User Provisioning

4.1 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 4.2 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 IT Operational Security Procedures.

No account belonging to an individual user is permitted to have a non-expiring password. Service accounts are permitted to have non expiring passwords where justified by the ICT Compliance Manager or Access Control.

No direct access to servers will be granted through a standard user account, access must only to be granted through the relevant Organisational Unit groups.

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 not permitted except when authorised by Access Control or IT Security and supported by a genuine business need (for instance a small number of third party and IT 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 must be removed upon system go-live.

Default administrator account passwords must be unique across the environment and changed when appropriate (e.g. when someone leaves).

4.2 Granting Access

All network accounts created (with the exception of test accounts with standard user privileges) must be authorised by an appropriate authoriser 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 (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 using a service request within the IT Service Management System.

SQL privileged accounts must be authorised by Data Management prior to access being granted. SQL privileges may be applied to a standard network account.

Third party access may only be granted following agreement of NECS Terms and Conditions and appropriate authorisation as outlined on the Third Party Service Access Request form.

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.

4.3 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 CCG organisations are the responsibility of respective managers. Managers must inform IT (via the relevant ICT Service Desk) of any amendment to be made to the privileges of their staff.

Any additional privileges must be approved before allocation.

4.4 Revoking Access

Monthly leavers reports must be sent from HR to IT to identify CCG users (for which HR support is provided) to be disabled.

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

4.5 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.

4.6 Re-enabling Disabled & Expired accounts

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

For an expiry date to be extended an appropriately authorised Account Amendment form must be submitted via the Service Management System.

5. Folder Access Management

5.1 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.

Access Control is the overall folder owner for all folders, as such any access may be authorised and/or removed where deemed necessary by Access Control.

5.2 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.

5.3 Information Classification

Where required Information will be classified in accordance with the NHS England Documents & Records Management Policy.

6. Access Reviews

6.1 Standard Network Accounts

Quarterly access reviews of standard user accounts must take place by Access Control.

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.

6.2 Privileged Network Accounts

A quarterly 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.

The following are mandatory groups to be included in the review to confirm the appropriateness of all members and service accounts belonging to the groups:

- Enterprise Administrators
- Built-in Administrators
- Domain Administrators

Any access found to be inappropriate must be amended in accordance with the NECS IT Change Management Procedure.

6.3 Folder Access

Folder access will be reviewed quarterly.

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

6.4 Authorisers

All approved authorisers within the IT Service Management System must be reviewed for appropriateness on a quarterly basis.

All Folder Owners must be reviewed by Access Control for appropriateness on a quarterly basis.

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

6.5 SQL access

Access to databases must be reviewed quarterly on a sample basis. Any users found to have inappropriate access shall have their access revoked,

6.6 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.

7. Password Management

All passwords must adhere to NECS standard as confirmed in the NECS IT Operational Security Procedures. 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 IT Operational Security Procedures.

Group policy password configurations will be reviewed at least annually to ensure adherence to the NECS IT Operational Security Procedures.

8. Physical Access

Physical Access to all NECS Sites is controlled to prevent unauthorised access, entry is controlled either via staffed or automated control points (e.g. swipe card access).

Areas hosting sensitive information and/or equipment have additional security measures in place and are restricted to authorised individuals only. Access is reviewed periodically.

9. Incident Reporting

Incidents must be reported in accordance with the NECS incident reporting policy and procedures.

10. Implementation and Distribution

This policy will be available to all staff for use in relation to access control management.

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.

11. Training Implications

The training requirements to comply with this policy are:

Induction training for Access Control. IT Service Desk, Systems and Security Staff to include access control processes.

Ongoing training for Access Control, IT Service Desk, Systems and Security Staff to ensure familiarity with access control processes.

12. Monitoring, Review and Archiving

12.1 Monitoring

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

12.2 Review

The sponsoring director will ensure that each policy document is reviewed in accordance with the timescale specified at the time of approval. **No policy or procedure will remain operational for a period exceeding two years without a review taking place.**

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

Whether or not the review results in changes to the document, the author will inform the Policy and Corporate Governance Lead who will schedule the revised policy for the next appropriate policy group meeting. Following re- approval, the policy will be re-issued under the next version number.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

12.3 Archiving

The Governance and Assurance Manager will ensure that archived copies of superseded policy documents are retained in accordance with Records Management Code of Practice for Health and Social Care 2021.

13. Documentation

13.1 Other related policy documents

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

- NECS IT Acceptable Use Policy
- NHS England Information Governance Policy
- NHS England Information Security Policy
- NHS England Documents & Records Management Policy

Further details on procedures are outlined in the following procedural documents:

- NECS Access Control Procedures
- NECS System Level Security Procedures
- NECS IT Operational Security Procedures
- Records Management Code of Practice for Health and Social Care 2021

13.2 Legislation and statutory requirements

This policy is written in adherence with the following requirements:

- Data Security and Protection Toolkit
- ISO27001 Standard

14. Appendix A

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 the 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: Click here to enter text.		

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	02/03/2021

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.