User Access Control Policy
Network Quarterly Data Collection (NQDC) application

1. Introduction

1.1. This Policy relates to the use of the Network Quarterly Data Collection (NQDC) application, hereafter referred to as ***the application***.

1.2. The purpose of the application is to enable the Health Innovation Network (HIN) to meet its reporting obligations to commissioners under the terms of the Master License Agreement, hereafter referred to as ***the business need***.

1.3. The application has been set up and is maintained by the Health Innovation Network (HIN) Informatics team at Health Innovation East, hereafter referred to as ***the Team***.

1.4. This Policy is written and maintained by the Team. It provides a framework for how user accounts and privileges are created, managed and closed.

2. Scope

2.1. This policy applies to all employees, third parties and suppliers who have access to the application:

- The HIN Informatics team
- HIN staff with access to the application to support the business need

3. Access principles

3.1. Access control standards have been established for the application to minimise information security risks and allow the organisation's business activities to be carried out without undue hindrance.

3.2. The standards will be reviewed by the Team not less than annually.

3.3. An audit log will be maintained to record user account creation, modification and closure.

3.4. All application users must have a HIN-issued email address and their user account will be attached to that email address.

3.5. Access to the application by individual users will be authorised by their HIN Metric Lead. Access will be terminated when no longer required to meet the business need.

3.6. Access will be allocated on the basis of business need and 'least privilege' in that users will only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

3.7. User access will be assigned using the role based access control (RBAC) model. All user accounts will be based upon job function and authorised by the HIN Metric Lead.

3.8. All access to information systems will be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user's identity.

4. Application administration

4.1. The Team will oversee management of the application and associated user accounts.

4.2. All user account procedures shall be performed only by suitably trained, certified and authorised application Administrators.

5. Applying for a user account

5.1. Request for a user account must be made by the member of staff's Metric Lead, by email to the Team at hininformatics@healthinnovationeast.co.uk

5.2. The Metric Lead must include the following core information about the member of staff:

- Full name
- Work email address
- The specific HIN to which access is required in the application
- Extent of access required
- Confirm the user will abide by the Acceptable Use Policy

5.3. All users will have a user ID for their sole use of the application. All individual user IDs will be unique for each user and never duplicated.

5.4. The Team Application Administrator will create the new account and store the request information in the audit log.

5.5. The Application Administrator will generate an email to the user with

- their user ID
- instructions to generate the password
- link to the application
- link to the Acceptable Use policy
- information that using the application indicates agreement the Acceptable Use policy

5.6. The new user will generate a password upon first sign in by requesting a password reset.

6. Modifying a user account

6.1. A user account must be modified if there is a change in the core user information provided.

6.2. Request for modifying a user account must be made by the staff's Metric Lead by email to hin-informatics@healthinnovationeast.co.uk including all core information:

- Full name
- Work email address
- The specific HIN to which access is required in the application
- Extent of access required

6.3. The Team Application Administrator will modify the account and store the request information in the audit log.

7. Managing a user account

7.1. The Team will initiate a review of all user accounts on a quarterly basis:

- The Application Administrator will produce a list of all active user accounts.
- The Team will email each Metric Lead with their respective accounts requesting confirmation that accounts are still required or if they should be closed.
- Metric Lead responses will be logged and closure requests actioned by the Application Administrator where required.

7.2. Plans for system monitoring will be reviewed after the penetration test.

8. Closing a user account

8.1. The Metric Lead must email the Team immediately it is known a user account is no longer required or within 3 working days of final required access, whichever is sooner.

8.2. The Team Application Administrator will close the account as soon as access is no longer required or within 3 working days of receiving a closure request, whichever is sooner.

8.3. Account closure may also be initiated by the Team in the event of application malfunction, inappropriate use or a suspected security breach. In this event, the Team will immediately inform the appropriate Metric Lead by email.

8.4. Administrator records closure in the audit log.

9. Breach of this Policy

9.1. Breach of this Policy may lead to the Team revoking access privileges to the application.

9.2. It may also result in disciplinary action up to and including dismissal or, in the case of a contractor, consultant, casual or agency worker, the termination of the engagement.

9.3. Users are required to co-operate with any investigation into suspected Policy breach.

Next review date: April 2026

Version	Amended content	Author	Date
Access Control Policy v1	New release	HIN Informatics team	May 2025
Access Control Policy v2	User Account Request Form includes acceptance of Acceptable Use Policy	HIN Informatics team	June 2025