NHS
Devon
Clinical Commissioning Group

Acceptable User Policy - privileged user

NHS Devon Clinical Commissioning Group

Owner(s): Amaresh Devarajan – IT Service and Cyber Security Manager	Directorate Contact Details: IT – D-CCG.IT@nhs.net	
Approved by: Data Protection Steering Group	Date of formal approval Oct 2021	Review Date: Oct 2022
Date Issued: Oct 2021		Version 2.0
All policies are held centrally by Governance: d-ccg.governance@nhs.net		

Document Change History:		
Version	**Date**	**Comments (i.e. reviewed/amended/approved)**
1.1	20/10/2020	Reviewed by Jim Goodwin, Shane Coe
2.0	21/10/2022	Reviewed: 5. Monitoring Compliance & Effectiveness updated and reworded.
2.0	28/10/2022	Ratified at DPSG

Equality, diversity and inclusion statement

NHS Devon CCG is committed to the promotion of equal opportunities, addressing health inequalities and fostering of good relations between people protected under the terms of the Equality Act 2010, the Health and Social Care Act 2012 and Human Rights legislation. We are equally committed to the elimination of unlawful discrimination, harassment and victimisation. To demonstrate this commitment, we develop, promote and maintain policies, strategies and operating procedures. Every effort is made to ensure that patients, employees, contractors or visitors do not experience discrimination; either directly or indirectly, because of their vulnerability; disadvantage; age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion and belief; sex (gender) or sexual orientation.

All staff must comply with this policy. Compliance must reflect our organisational commitment to and policy on, equality, diversity and inclusion. In addition, each manager and member of staff involved in implementing this policy must give due regard to the needs of those protected under law.

If you, or any other groups, believe you are discriminated against under the terms of the Equality Act, the Health and Social Care Act 2012 or Human Rights legislation by anything contained in this document; or you need this document in an alternative format, for example, large print, Braille, Easy read or other languages; please contact our Patient Advice and Complaints Team (PACT):

Tel: 0300 123 1672
Email: pals.devon@nhs.net,
Post: Patient Advice and Complaints Team,
FREEPOST EX184,
County Hall,
Topsham Road
Exeter
EX2 4QL

Contents		
Section	**Title**	**Page**
	Introduction	4
1	Scope of Policy	4
2	Definitions	4
3	Responsibilities	5
4	Statutory Basis	6
5	Monitoring Compliance and Effectiveness	6

Introduction

Analyst and developers in Business Intelligence (BI) team have privileged access to some IT systems that may pose higher data and cyber security risks. The privileges they have with respect to business systems, endpoints, data warehousing systems, data modelling, data analytics and application development are for the express purpose of Business Intelligence department functions. The purpose of this Policy is to establish requirements for acceptable use of privilege access for analysts and developers in BI team.

1. Scope of Policy

This policy applies to all members of the Business Intelligence team who require higher than normal privileges to NHS Devon CCG IT systems. Examples of these types of privileged access include; the ability to download and install applications, install packages, use software development tools, ability to compile software code, access to data warehousing databases, ability to create data models using data warehousing. Anyone with these or other enhanced privileges is responsible for adhering to this policy.

Delt Shared Services and the NHS Devon CCG Digital team have the right to perform activities to audit, test, and investigate the access and actions of these B.I staff and their devices in order to ensure that security protections and I.T security controls are maintained.

2. Definitions

Privileged Access – Is a type of I.T access that allows users access to sensitive systems with elevated permissions than typical users;
Endpoints – Is any computing device that is connected to I.T network with access systems and applications;
Packages – Collections of files, software's, other resources which collectively provides desired functionality;
Data warehousing – Is an electronic storage where collection of sensitive business data is stored;
Data modelling – Process where complex structured data is documented and interpreted for ease and business needs;
Compile software code – Is an activity that software developers initiate to transform human readable language to computing language;
Development tool – Is an application that developers use create customised tools and applications;

3. Responsibilities

1. Restrict their use of accounts with privileged access to only official NHS Devon CCG business, consistent with the analytics, development and data modelling job responsibilities, and the purpose for which the access was granted. Users may not use their privileged access for any purposes outside of the scope for which such privilege access was granted.

2. Never share their login credentials.

3. Never download and install any packages, plugin, addons, application and other software's from the Web without prior approval from Delt cyber security team through the current Delt I.T request management process.

4. Never knowingly or unknowingly download and install of any packages, plugin, addons, application and another software from the Web that may pose security risk to data, services, threat to systems hosted by DELT I.T services and/or by NHS Devon CCG.

5. Never gain or provide unauthorised access to an I.T System. System Administrators must never give themselves or another user access to I.T Systems that they have not been formally authorized to access.

6. Ensure that security controls are not circumvented by way of actions taken by the developers or individuals accessing developer's systems.

7. Never use Privileged Access to satisfy personal curiosity.

8. Never configure their systems to bypass security controls, including, without limitation, the installation of programs or services that allow the systems to be managed or accessed insecurely or through unauthorised means

9. Ensure that default passwords are changed using strong password methodologies when they install or build any components as part of their role.

10. Never allow other users or systems to conduct security audits or tests against or through Delt or NHS Devon CCG I.T systems or networks without coordination with and the explicit, written consent of an authorised officer of Delt cyber security team.

11. Never gain unauthorised access or attempt to gain unauthorised access to Delt or NHS Devon CCG networking, security, management, backup, storage or monitoring systems

12. Never install programs or configure systems to allow 'sniffing' or other network traffic capture or analysis.

13. Never access or attempt to access security-relevant information, such as password files that may, among other things, be used to gain unauthorised access to system accounts.

14. Never install or use software for the purpose of cracking encrypted data, including, without limitation stored passwords.

15. Maintain and provide Delt cyber security team with a list of authorised individuals and accounts that are permitted to have admin and/or enhanced permissions on systems hosted by Delt services

16. Notify Delt IT services in writing if a user no longer requires admin and/or enhanced level permissions on any systems that below to NHS Devon CCG. To ensure that access is deleted or revoked on time, Delt IT services must receive this notification at least five business days in advance of the date that the access is no longer needed by that individual.

17. Assume all responsibility for the consequences of the use of their respective account by an unauthorised individual.

4. Statutory Basis

Implementation is part of the organisation requirement for ongoing compliance with the National Data Guardian Security standards, as outline below:

Data Security Standard 2:
All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 5:
Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

5. Monitoring Compliance and Effectiveness

Our security system continually analyses new passwords against banned or compromised passwords to keep the most vulnerable passwords out of our systems. Some examples of banned passwords e.g. Password1234$, DevonCCG123$, QWERty123$

For more information please contact d-ccg.it@nhs.net