NHS Confederation

# IT Security Policy

Charity number 1090329

Company number 04358614

| | |
|---|---|
| Owner of policy | Director of Finance and IT |
| Date of policy review | May 2024 |
| Date of next review | May 2025 |
| Approved by CEO | 10th June 2024 |

## Contents



Version Control:

| Version | Date | Changes |
|---|---|---|
| 1 | March 2019 | New policy |
| 2 | October 2023 | Reviewed and updated and approved by the Board |
| 3 | May 2024 | Reviewed and updated, significant changes |
| | | |

## 1. Purpose and scope

The purpose of this policy is to set out the NHS Confederation's approach to IT Security.

NHS Confederation provides hardware and software intended to support and empower employees in the performance of their duties. There are many technical controls in place to protect our organisation. Whilst the organisation has layered security controls around our IT systems, it is important for end users to actively play their part in maintaining IT security.

This policy intends to protect NHS Confederation's information, assets, and reputation. It applies equally to every employee or user (contractors, trustees, external guests etc) logging on to NHS Confederation's IT equipment or accessing NHS Confederation's IT systems.

Failure to comply with this policy may result in disciplinary action.

## 2. System Access Management

2.1 Access to our electronic systems runs parallel with the joiner, leaver, mover process. All newly created accounts are created based upon the principle of least privilege. No accounts are active or created until the necessary employment checks have been completed and a signed contract is received by HR (employees, secondees and volunteers) or the contracting team (consultants).

2.2 Temporary and supplier access accounts need to be authorised and approved by the Head of IT or included in the supplier contract. These accounts must automatically expire after a predetermined time or be manually terminated when no longer required.

2.3 Local admin account passwords will not be shared with staff unless for emergency or break-glass scenarios, after which, the local admin password will be changed.

2.4 Changes to system access require authorisation from the system owner and line managers prior to users gaining access.

2.5 Where a colleague needs to access another user's 365 account whilst the user is absent, for example Outlook and OneDrive, a request should be made to the Head of IT who will liaise with both the Director of People and Governance and the Director of Finance and IT if required before access is granted.

2.6 Access using administrator privileges are monitored and logged using Microsoft Defender. Defender sends alerts to the Stripe SOC team who investigate to ensure the activity is business as usual (e.g. Stripe being given admin rights to carry out work). Admin privileges are also reported to the Director of Finance and IT as part of the QBR meeting. See more detail on this in Section 4 below.

2.7 Access to all systems and applications is controlled by password and multi factor authentication. Any exception to this rule should be highlighted in the DPIA and the appropriate risk assessed.

2.8 Log in from outside of the UK is prohibited unless approved by the Director of Finance and IT, or another Director if the Director of Finance and IT is on

leave/absent. All approved requests are shared with the SOC team to allow access though all log ins without approval will be blocked.

## 3. Multi-Factor Authentication (MFA) and Passwords

3.1 Multi-factor Authentication is used to identify users for access to electronic systems in more than one way.

3.2 Single Sign On protocols are in place, where possible, to allow access to internal systems if a secure connection is already authenticated.

3.3 Users of NHS Confederation electronic systems, shall be uniquely identified, authorised, and authenticated using MFA.

- Passwords are required for each user to be able to access the Confederation systems. We follow password management best practice which advises passwords should not be frequently changed. However, it does mandate: minimum 12 characters and must include upper case letters, lower case letters, numbers and special characters.

- The use of three random words is a recommended approach and familiar names such as pets, children and siblings along with repeated passwords and added numbers are to be avoided.

- In addition to passwords, another authentication method is required. Typically, this will be provided via the Authenticator App, which can be downloaded from the company portal

3.4 To ensure the highest levels of security possible, all users are reminded that all passwords for the network and software are not to be shared with anyone else, either inside or outside of the organisation. Sharing your password may lead to disciplinary action.

3.5 Passwords should not be left on labels or written on the outside of devices including when kit is being returned to the organisation.

3.6 If you believe that your password has been compromised or someone else has been using your login details, change your password immediately and advise the SOC team at Stripe security.alerts@stripeolt.com or 0117 974 6229.

3.7 Stripe monitor log in and access 24/7 and if they suspect a compromised account, they can block any attempts to sign in. In this scenario, Stripe will contact the Head of IT to investigate and advise what action to take.

3.8 Non-windows laptop mobile devices e.g. tablets and phones, are managed by the Confederation's Mobile Device Management tool which will ensure security compliance. There will be a requirement to have at least a 6-digit passcode for any

mobile device as part of the initial set up. Passcodes must be non-consecutive numbers.

## 4. Privileged Access Management (PAM)

4.1 Privileged and super user accounts should only be used for system administration purposes. In M365 applications, only members of the in-house IT team and colleagues at Stripe can be given access at this level.

4.2 In M365, all privileged actions are monitored and logged using PAM tooling, for example:

i) actions taken by any individual or shared account with root or administrative privileges.
ii) access or modification attempts to any log or audit files.
iii) actions taken which affect the ability to collect audit data, including the stopping, starting and pausing of logging service on any application, system or device.
iv) creation and deletion of system-level objects.

4.3 For all M365 and Microsoft cloud applications, privileged functions (such as system administrators) must use separate logon accounts when performing those privileged functions. General computing activities such as internet browsing and email must be performed from user's primary, non-privileged account.

4.4 The use of local privileged accounts must be authorised by the Head of IT.

4.5 Audit logs capture privileged actions in all non-M365 systems.

## 5. Data Processing Impact Assessments

5.1 In line with Cyber Essentials Plus accreditation, all new systems and applications, or major changes to existing systems, must have a Data Processing Impact Assessment (DPIA).

## 6. Physical security for IT Comms Rooms

6.1 IT security controls include the physical controls in place to prevent unauthorised access to our IT Comms Room. The IT Comms Room doors must be closed and locked at all times.

6.2 Staff members should not allow access to our IT Comms Room to any individual without first identifying them and confirming why they require access and then logging them into the daily sign in sheet.

## 7. Guest Protocols

7.1 No external devices are allowed to connect to the NHS Confederation network systems with the exception of connectivity to meeting room TV audio IT equipment which is not connected to the network.

7.2 Guests attending our office space should be allocated to the Guest Wi-Fi and not given access to any network IT equipment.

## 8. VPN

8.1 Users who need access to the internal file shares (Z/P drive) need to use the Cisco AnyConnect VPN to do so.

8.2 VPN creates a secure tunnel to access these files and is only required to perform these tasks when working remotely and requiring access to the internal file shares. It is not required for all users as this inhibits the Stripe SOC team in monitoring and tracking of geolocations.

8.3 The Head of IT will keep all staff advised of changes and updates to VPN and when it is no longer required to be used.

## 9. Responsibilities

### 9.1 Group Executive

i) Supporting and leading a top-down approach to Information and IT security i.e leading by example
ii) Completing all mandatory training and following up with staff teams to complete mandatory training as necessary
iii) Ensuring software used within the Department is appropriate and authorised in line with the Software Policy and any admin rights held within the team are transferred in the event of that user leaving or moving roles.

### 9.2 Senior Information Officer - Director of People and Governance

i) Is legally responsible for setting the organisation's data protection policy, ensuring compliance against it.
ii) Managing the Confederation's business continuity planning and co-ordinating responses to significant incidents.

### 9.3 Chief Information Technology Officer - Director of Finance and IT

i) Is responsible for cyber security to maintain the confidentiality, availability, and integrity of electronic information systems.
ii) ensuring there are controls in place to prevent data being breached by providing a layered security approach to our environment (including firewalls, MFA etc) and ensuring protection of information during communication and daily operations.
iii) ensuring all staff members are aware of IT policies by covering annual policy awareness and guidance on information security.
iv) Working with Stripe OLT the Confederation's managed service provider ("Stripe") to oversee authorisation to systems and hardware including access from locations outside of the UK.
v) Approving access to our systems (new starters, changes, leavers) and ensuring access is given with least privilege.
vi) Approving access to applications and systems.

### 9.4 Head of IT

i) Responsible for developing and implementing the IT Security Policy.
ii) Responsible for ensuring the organisation's IT systems and policies align with Information Governance Policies.
iii) Is the Business Continuity lead for IT.
iv) Responsible for the management and communication of the Disaster Recovery Plan.
v) Input to Data Processing Impact Assessments (DPIA) for project work.
vi) For inputting into all large-scale IT related projects (including but not limited to the CRM or Finance / HR systems) to ensure privacy by design.
vii) Ensuring retired assets are wiped and securely disposed of.
viii) Monitor and report on mandatory training to raise awareness of IT security.
ix) To manage the auditing process to check permission levels, ensuring account changes are actioned throughout the joiner, leaver and mover process.

### 9.5 Office Management Team

i) Keep a register of guest access to offices.
ii) Ensure door entry and logs are maintained.

### 9.6 Stripe OLT - MITSA

i) Maintaining our infrastructure and liaising with NHSC staff to manage any vulnerabilities discovered by the SOC team
ii) Continuous monitoring of network health and patching.

iii) Managing hardware set-up and software configuration.
iv) Managing access permissions and gaining approval from line managers, Head of IT (or delegate), where requests for elevated privileges are received.
v) Configuring conditional access policies in our technical environment.
vi) Implementing Disaster Recovery Plan when required.
vii) Creation of user accounts in a timely manner, supported by approved documentation.
viii) Managing and monitoring all generic, shared and group accounts with regular reviews with NHS Confederation staff to ensure the accounts are still active.

### 9.7 Stripe OLT - Security Operations Centre

i) Blocking access from untrusted locations.
ii) Management of the security posture.
iii) Regular phishing campaigns and related staff training.
iv) Blocking, investigating and reporting any incidents or attempted security breaches.
v) Reporting on and improving Data Loss Protection processes.
vi) Monitoring our systems access including administrative access and ensuring logs of changes to access are maintained.
vii) Proactive vulnerability assessments to endpoint devices and systems, and reporting to MITSA for remediation.
viii) Road mapping security improvements.

### 9.8 Stripe OLT - Account management team

i) Delivering the quarterly business review meetings

### 9.9 Line manager responsibilities

i) Ensuring your team have read and understand their responsibilities within this policy.
ii) Completing a new starter form, in line with the new starter process, ensuring permissions requested and hardware requests are appropriate to their role and with minimum privilege in mind.
iii) Approving any changes to permissions for our team members.
iv) Notifying the Head of IT when employees are leaving the organisation using the leavers form on Cascade ensuring the return of IT equipment provided by NHS Confederation by the last day of employment to ensure accounts are closed and access is removed.
v) If third parties (e.g. secondees, consultants or volunteers) are given access to the network, it is the responsibility of the recruiting manager to inform them about this policy and the manger should inform the Head of IT when access should be removed.

### 9.10 All staff responsibilities

i) Being aware and complying with each of the IT policies.
ii) Completing appropriate mandatory training.

iii) Users are responsible for managing the devices provided to them by the organisation. This includes locking devices when leaving them unattended and not allowing your device to be used unsupervised by another user.
iv) Ensuring all provided kit is taken care of, stored in a secure location and is not accessible by unauthorised users, including family members and other members of staff.
v) Ensuring the timely return of all redundant kit to ensure secure disposal including items of IT equipment no longer required for your role.
vi) Reporting lost or stolen equipment immediately to their line manager and Head of IT, and where appropriate provide a crime reference number.
vii) Ensuring guests entering our office locations are accompanied at all times.
viii) Adhere to the policy guidance on password use and storage i.e. not sharing or disclosing passwords to any other person or documenting on the device.
ix) Following guidance to protect against virus infection and phishing attempts by reporting suspicious emails using the 'Report Phishing' button in Outlook and not forwarding or opening anything suspicious.
x) Not opening email attachments from unknown or unreliable sources.
xi) Monitoring large distribution lists and ensuring that information is shared only with an intended audience.
xii) Ensuring all security updates are applied to all devices by restarting devices when prompted by Stripe OLT and complying with any mobile device updates.
xiii) Ensuring all data is stored in locations provided by the organisation and not to forwarded or stored in any non-corporate repository or personal email accounts including unencrypted USB sticks (or only using encrypted USB sticks authorised by IT).

# Equality Impact Assessment - Policies

The following guidance and checklist provides a framework for Equality Impact Assessments (EIA). It should be used when carrying out equality impact assessments (EIA) in relation to any new or revised policy. The checklist will help in considering the impact of the policy in relation to equality and diversity (E&D).

The Checklist is to be used for any new or revised policy, not just those that appear to have high relevance in relation to equality and diversity issues. Completion of the Checklist does not need to be a time-consuming or difficult process but should raise some important questions as you carry out the process.

| | |
|---|---|
| Name of policy being assessed | IT Security Policy |
| Policy Owner | Director of Finance and IT |
| EIA completed by | Director of Finance and IT |
| Date Completed | May 2024 |
| Summary of purpose of the policy | To provide guidance around IT Security |
| Who are the main stakeholders and what involvement and consultation have they had in the policy development. Include staff groups, trade unions and board committees as applicable. | All staff working with and on behalf of NHS Confederation |
| Who is affected by the policy | All staff and users |

| | |
|---|---|
| What are the arrangements for monitoring and reviewing the actual impact of the policy | QBR reporting from Stripe OLT.<br><br>Continuous monitoring of our systems and networks.<br><br>Reporting to ARC. |

Please indicate against each of the following protected characteristics, what the impact of the policy would be and actions that will be / have been taken to mitigate any negative or adverse impact identified.

(Where the policy is found to have either a positive or negative impact on a particular group it will need to be reviewed or justified within the permits of the law.)

| Protected Characteristics | Impact Y/N | Action(s) you will take to mitigate or remove the negative or adverse impact if identified? | Action Owner |
|---|---|---|---|
| **Age**<br>*Consider impact on young people, older people etc.* | N | | |
| **Disability**<br>*Consider people with physical disabilities, hidden disabilities and neurodiversity.* | N | | |
| **Gender Reassignment**<br>*Consider people undergoing or have undergone gender reassignment* | N | | |
| **Pregnancy and Maternity**<br>*Consider those who are pregnant and those on pregnancy and parenthood leave. Consider those wishing to take parenthood leave* | N | Options for staff on maternity leave – 1. asked to reboot laptop once a month or 2. surrender kit. | NB/MP |
| **Race / Ethnicity**<br>*Consider potential impact on people from different ethnic groups and nationalities.* | N | | |
| **Religion or Belief**<br>*Consider people with different religious, faith and non-beliefs* | N | | |
| **Gender**<br>*Consider all genders.* | N | | |
| **Sexual Orientation**<br>*Consider LGBTQ+ people.* | N | | |
| **Marriage and Civil Partnership** | N | | |

| | | | |
|---|---|---|---|
| *Consider marriage and civil partnership in respect of the due regard to the need to eliminate unlawful discrimination in employment.* | | | |
| Does the policy promote fairness and equal opportunities? Provide details. | Yes, the policy is applicable to all workers equally and fairly | | |

| | |
|---|---|
| Manager Signature: NBarraclough | HR Review Signature: MPritchard |
| Date:10.6.24 | Date: 10.6.24 |