South East Coast Ambulance Service NHS
NHS Foundation Trust

Remote Access Policy

Contents

1 Statement of Aims and Objectives

1.1. The Trust recognises that there are significant benefits in allowing staff and suppliers the flexibility to access the Trust's networks remotely.

1.2. The measures described in this policy will permit authorised staff and suppliers to access the Trust's networks remotely in a secure and controlled manner.

1.3. This policy addresses information security issues relating to the provision of remote access to staff. Any Health and Safety obligations the Trust may have in relation to home workers falls outside the scope of this policy.

1.4. This policy covers all types of remote access, whether fixed or 'roaming' including:

1.5. Mobile staff working from non-Trust sites;

1.6. Staff working from home temporarily or permanently;

1.7. Non-NHS staff (e.g. third-party suppliers);

1.8. The objectives of the Trust's policy on remote access

1.9. To provide secure and resilient, named and role-based remote access to the Trust's information systems;

1.10. To preserve the confidentiality, integrity and availability of the Trust's information and information systems;

1.11. To mitigate information security risks that may result in serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security;

1.12. To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Trust is adequately protected under computer misuse legislation.

2 Principles

2.1. Remote Access refers to any technology that enables the South East Coast Ambulance Service NHS Trust ('the Trust') to connect approved users in geographically dispersed locations.

2.2. This access is typically over a securely managed Virtual Private Network (VPN), Access Point Name (APN), 4G/5G mobile data networks or the Internet.

2.3. The security architecture is integral to the Trust network and comprises password and multi-factor authentication, authorisation, monitoring and accounting.

2.4. To ensure the most comprehensive level of protection possible, the Trust's networks include security components that address the following five aspects of network security:

2.4.1. **User Identity** - All remote users must be registered and authorised by the IT department. User identity will be confirmed by user ID and password/multi-factor authentication wherever possible, and a log kept of all user remote access;

2.4.2. **Perimeter Security** – Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass in and out of the network. Routers and switches handle this access control through access control lists and dedicated firewalls. Firewalls provide a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, in accordance with the Network Security Policy. Complementary tools, including virus scanners, proxies and content filters, are utilised to manage traffic that is allowed into the network perimeter.

2.4.3. **Secure Connectivity** - The Trust will protect line of business, confidential and person identifiable data from eavesdropping or tampering during transmission using industry standard encryption mechanisms.

2.4.4. **Security Monitoring** – Firewall, router and traffic monitoring software and services will be used to identify areas of weakness and respond to security events as they occur.

2.4.5. **Remote Diagnostic Services and Third Line Support Parties** – Software and hardware suppliers will be required to have secure remote access to such systems by request or on demand to upgrade, provide monitoring or analysis services or investigate and fix faults. The Trust will have appropriate contracts and a Data Sharing Agreement or Information Sharing Protocol in place.

2.4.6. **Geo-blocking** - Geo-blocking is technology that restricts access to Internet content based upon the user's geographical location. The Trust limits remote access for all countries outside of the UK. Exceptions to this rule for users or third parties must be approved by the SIRO and IT Security Manager.

2.5. Staff with an active network account and a Trust provisioned laptop will be provided with a secure remote access capability using appropriate Trust approved VPN software. No attempt must be made to circumvent that secure access.

2.6. Staff with an active network account and a Trust provisioned tablet will be provided with a secure remote access capability using a Mobile Device Management software tool.

2.7. Third parties requiring secure remote access will need to provide a completed Remote Access Application submitted by the Trust business

owner, Information Access Owner (IAO) or representative, of the system requiring access via Marval.

2.8. Approved third parties will be provided with remote access that needs to be activated by the IT department on request.

2.9. Some third parties require on-demand remote access to ensure minimum delay in resolving issues for business-critical applications. This type of connection should be requested and validated at time of application.

2.10. Third party access will be provided via a Privileged Access Management (PAM) system. PAM is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources.

3 Responsibilities

3.1. **The Chief Executive Officer** (CEO) is ultimately accountable for the implementation of this Policy.

3.2. **The Trust Board** have responsibility to obtain assurance that the processes described work effectively and support the Board level public commitment to implementation of the Remote Access Policy

3.3. **The Director of Finance** is responsible for ensuring that remote access by staff and suppliers is managed securely.

3.4. **The Compliance Working Group** (CWG) will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to mitigate those risks.

3.5. **The Associate Director of Information Technology** is responsible for confirming whether remote access to business applications and systems is appropriate and permitted.

3.6. **The Head of Infrastructure & Networks** will have responsibility for each remote access connection to ensure that the Trust's policy and standards are applied.

3.7. **The IT Security Manager** will ensure that all applications are approved in accordance with the Remote Access Policy and the Network Security Policy.

3.8. **The Head of IT Service Delivery** will ensure that approved applications are provided in a timely manner and in accordance with this policy.

3.9. **The IT Network Specialist** will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels and access is recorded.

3.10. **The Information Security and Registration Authority Manager** will provide advice on assessing information security risks and ensure that controls are being applied effectively.

3.11. All remote access users are responsible for safeguarding Trust equipment and information resources and notify the Trust immediately of any security incidents and breaches.

3.12. Staff and suppliers must return all Trust equipment on termination of the access arrangements or on termination of contract or employment.

3.13. All parties provided with remote access must adhere to Trust policies and procedures governing the appropriate use of computer equipment; email and Internet use; and management of confidential, person identifiable or otherwise sensitive information.

3.14. Staff who access their email account or document storage remotely may not download or print content containing person-identifiable or sensitive information to non-Trust equipment.

4 Competence

4.1. As part of statutory and mandatory training, the Trust will ensure that all staff are provided with the necessary security guidance and awareness to fulfil their responsibilities in relation to data protection, confidentiality and information security.

5 Monitoring

5.1. The Information Security and Registration Authority Manager will monitor compliance with this policy as part of the annual system of information security audits. Where the Trust deems appropriate, internal audit will be asked to conduct information security audits.

6 Audit and Review

6.1. The IT Security Manager and IT Manager - Service Desk will review all applications for remote access submitted via the IT Service Desk.

6.2. All connections into the network will be recorded for audit purposes and an alert sent to relevant IT staff.

6.3. The document will be reviewed every three years unless changes in legislation or working practices require an earlier review.

6.4. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

6.5. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

7 References

- Confidentiality: NHS Code of Practice
- Data Protection Act 2018
- Computer Misuse Act 1990
- ISO/IEC 17799:2000

8 Glossary

- Trust – The South East Coast Ambulance Service NHS Trust
- VPN – Virtual Private Network
- APN – Access Point Name
- GSM – Global System for Mobile Communications
- GPRS – General Packet Radio Service
- CWG – Compliance Working Group
- DSA – Data Sharing Agreement
- ISP – Information Sharing Protocol
- NDA – Non-Disclosure Agreement

Appendix A: Application for Remote Access

Please use this form to submit any requests to the network team and allow sufficient time for the request to be assessed and recorded for audit purposes.

All fields are mandatory.

Requestor:	
Department:	
Contact Number:	
Service Desk Reference:	
Date of Request:	
Date Required (if applicable):	

Supplier Name:	
Reason for Access:	
Names/IP's of SECAmb End Points:	
Account Name (if known):	
Always-On Connection Required:	Y / N
Always-On Justification:	

For Completion by IT:

NDA/DSA/ISP Completed:	NDA ☐ DSA ☐ ISP ☐