East of England Ambulance Service NHS Trust

Remote Access Policy

Document Reference:	POL054
Document Status:	Approved
Version:	V4.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IT	February 2013	IM&T Security & Resilience Manager
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
3.1	April 2019	A Marrs
3.2	May 2019	Approved at IGG
4.0	June 2019	Approved by MAG

Document Reference	
Recommended at **Date**	Information Governance Group 15th May 2019
Approved at **Date**	MAG 14th June 2019
Review date of approved document	May 2021
Equality Impact Assessment	February 2019
Linked procedural documents	N/A
Dissemination requirements	All Trust Staff
Checklist Complete	Yes
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual

workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Paragraph **Page**

Appendices

1. Introduction

Remote Access refers to any technology that enables you to connect users in geographically dispersed locations to files and Trust systems. Often business processes rely on easy and reliable access to corporate information systems. In practice, the benefits of securing remote access are considerable – business can be conducted remotely with confidence and sensitive corporate information remains confidential.

This policy covers all types of remote access:

- Travelling users (e.g. Staff working temporarily based at other locations)
- Home workers (e.g. IM&T support, Corporate Managers, Clinicians)
- Non NHS staff (e.g. contractors and other 3rd party organisations)

2. Purpose

This document sets out the policy for remote access and includes a set of common controls, which can be applied to reduce the risks associated with a remote access service.

The objectives being:

- To provide secure and resilient remote access to the Trust's information systems
- To preserve the integrity, availability and confidentiality of the Trust's information and information systems

- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security
- To comply with all relevant regulatory and legislative requirements (current data protection legislation and to ensure that the Trust is adequately protected under computer misuse legislation

3. Duties

3.1 Head of IM&T

Is ultimately responsible for ensuring that remote access by staff is managed securely.

3.2 IM&T Department

Will maintain policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.

3.3 All Remote Access Users

Are responsible for complying with this policy and associated standards. They must safeguard corporate equipment and information resources, notify the Trust immediately of any security incidents and breaches.

3.4 Consultation and Communications with Stakeholders

Consultation will be via the departmental and staff representatives on the Information Governance Group, and when agreed will be communicated to all staff.

4. Definitions

Remote Access – please see section 1 Perimeter Security – External facing technical solutions designed to prevent unauthorised access to Trust resources.

5. Development

5.1 Prioritisation of Work

This policy is required as part of the Trust's wider security requirements, and details the requirements outlined in the Information Security and IM&T Operational Security policies.

5.2 Identification of Stakeholders

Stakeholders are all Trust staff.

5.3 Responsibility for Document's Development

The development of this document is the responsibility of the IM&T Security and Resilience Manager, in conjunction with other senior technical managers.

6. Connectivity

6.1 Perimeter Security

The Infrastructure Team will be responsible for ensuring perimeter security solutions are in place and operating properly. Perimeter security solutions will control access to critical network applications, data, and services. Remote Access solution(s) must be secure, therefore when connected all traffic must be via the Trust network and clients must not be able to access local resources. Authentication must be two factor, of which one factor must be a user account, and the other a unique dialer account.

6.2 Security Monitoring

Network vulnerability systems will be used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

6.3 Remote Diagnostic Services and 3rd Parties

Suppliers of central systems/software that require remote access to systems will be permitted subject to it being initiated by the computer system and all activity monitored.

Each supplier or Trust user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives. Each request for remote access will be authorised by approved IT staff, who will only approve access when satisfied of the need.

7. Equality Impact Assessment

This is attached, Executive Summary is in Appendix C

8. Dissemination and Implementation

8.1 Dissemination

This policy will be held in the document library and advertised in line with the Trust policy on dissemination of procedural documents. It will be circulated within IM&T via the senior management team

8.2 Implementation

Technical and environmental implementation is currently in place in line with this policy, current legislation and best practice.

9. Process for Monitoring Compliance and Effectiveness

Audits will be conducted periodically to ensure these procedures and protocols are being adhered to, failure to comply with these procedures and/or protocols will be deemed as a failure to comply with the policy and may therefore be treated as a disciplinary matter. All security weaknesses and incidents must be reported to the IM&T Security & Resilience Manager through the IM&T Service Desk, and logged on the Trust's incident management system.

10. Standards/Key Performance

Indicators Audits will be conducted periodically to ensure these procedures and protocols are being adhered to, failure to comply with these procedures and/or protocols will be deemed as a failure to comply with the policy and may therefore be treated as a disciplinary matter.

11. Associated Documents

Information Security Policy

IM&T Operational Security Policy

Appendix A –Equality Impact Assessment

EIA Cover Sheet		
Name of process/policy	IM&T Remote Access Policy	
Is the process new or existing? If existing, state policy reference number		
Person responsible for process/policy	IT Security & Resilience Manager	
Directorate and department/section	Strategy & Sustainability	
Name of assessment lead or EIA assessment team members	IT Security & Resilience Manager	
Has consultation taken place? Was consultation internal or external? (please state below):	Via email	
Internal	Head of IM&T	
	Deputy Head of IM&T	
	IT Infrastructure Service Delivery Manager	
	IT Service Desk Service Delivery Manager	
The assessment is being made on: Please tick whether the area being assessed is new or existing	Guidelines	**X**
	Written policy involving staff and patients	
	Strategy	
	Changes in practice .	
	Department changes	
	Project plan	
	Action plan	

	Other (please state) Training programme	

EQUALITY ANALYSIS					
What is the aim of the policy/procedure/practice/event? Defines the policy for remote access.					
Who does the policy/procedure/practice/event impact on? Nobody					
Race		**Religion/belief**		**Marriage/Civil Partnership**	
Gender		**Disability**		**Sexual orientation**	
Age		**Gender re-assignment**		**Pregnancy/maternity**	
Who is responsible for monitoring the policy/procedure/practice/event? IT Security & Resilience Manager					
What information is currently available on the impact of this policy/procedure/practice/event? None					
Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? No					
Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No, If yes please provide evidence/examples:					
Race		**Religion/belief**		**Marriage/Civil Partnership**	
Gender		**Disability**		**Sexual orientation**	
Age		**Gender re-assignment**		**Pregnancy/maternity**	

Please provide evidence:

No

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? Yes/No, if so please provide evidence/examples:

Race		**Religion/belief**		**Marriage/Civil Partnership**	
Gender		**Disability**		**Sexual orientation**	
Age		**Gender re-assignment**		**Pregnancy/maternity**	

Please provide evidence:

No

Action Plan/Plans - SMART

Specific
Measurable
Achievable
Relevant
Time Limited

None required

Evaluation Monitoring Plan/how will this be monitored?

Who
How
By
Reported to Head of IM&T

There is zero impact on any "characteristic" therefore there is no need to monitor.