Remote Access Policy

Document Reference	POL054
Document Status	Approved
Version:	V3.0

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)**
1.0	Feb 2013	Approved by Executive Management Team
2.1	March 2015	Reviewed by A Marrs
2.2	July 2018	Approved by Information Governance Group
3.0	March 2019	Approved by Management Assurance Group

Document Reference	
Recommended at Date	Information Governance Group 11th July 2018
Approved at Date	Management Assurance Group March 2019
Valid Until Date	July 2021
Equality Analysis	Completed
Linked procedural documents	N/A
Dissemination requirements	All Trust staff
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

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.

6.4 Non Trust Owned Devices

Data can only be stored on encrypted equipment owned and supplied by the Trust. Attempting to setup access on any device that results in data being stored on that device, may result in disciplinary action. An exception is in place for personal mobile phones and tablets whereby they are permitted to connect to the Trust email system. The configuration details for this must be requested via the IM&T Service Desk standard procedure.

The device must be encrypted to conform to Trust and National policy. Encryption is activated automatically with Smartphones (iPhones, Android, Nokia, etc.) and a passcode enforced when connected to an Exchange server.

Staff must be aware that by configuring personal devices to receive Trust email they are automatically allowing IM&T to control your device. This is purely for security purposes, IM&T cannot access personal devices or the information on it. However, IM&T will have the ability to remotely wipe personal devices completely should they be lost or stolen. The device will be reset to factory settings if this is necessary. Staff have a duty to inform IM&T as soon as possible should your device be lost or stolen. If staff are not happy for IM&T to have this ability then they should not configure personal devices to receive Trust email. Staff will still have the ability to connect to Trust email using the web browser on your personal devices without any configuration required and without giving IT the ability to remotely wipe the device. Staff should note that although using personal devices to connect to Eastamb email is permitted; the device, it's connectivity and configuration are not supported by IM&T. Should staff need assistance with setting personal devices up they should seek assistance from their mobile providers.

Connection to the Trust email is permitted via the Internet from all connected devices via Outlook Web Access, the connection details for this must be requested via the IM&T Service Desk standard procedure. When using this facility staff must not allow browsers to store any logon details.

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

Appendices

Appendix A	Document Checklist
Appendix B	Monitoring Table
Appendix C	Equality Impact Assessment: Executive Summary

Appendix A – Document Checklist

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	**Y**	
2.	**Definitions**		
	Have all key terms been clearly defined?	**N/A**	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	**Y**	
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	**Y**	
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	**Y**	
6.	**References/Associated Documents**		
	Are key references cited?	**Y**	
	Are linked documents identified where appropriate?	**Y**	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	**Y**	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Y**	
	Does the plan include the necessary training/support to ensure compliance?	**Y**	
8.	**Review Date**		
	Is the review date identified?	**Y**	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name		Date	
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	

Appendix B – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Remote access to Trust resources	IM&T Infrastructure and System staff	System log files	Monthly A report to IM&T Senior Managers will be produced on request, or when an incident has occurred	Connectivity report exported from the remote access system	Reports will be sent to the requesting manager, in all cases reports should be copied to the IM&T Security & Resilience Manager	The IM&T Management Team will evaluate and issue subsequent recommendations and action plans for any or all identified deficiencies, breaches of policies, or improvements	Changes to policy and/or improvements will be implemented in line with the IM&T change control process, lessons learned will be shared with IM&T operational staff and Estates.

Appendix C - Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference:	Document Title: Remote Access Policy
Assessment Date:	Document Type: Policy
Responsible Director: CIO	Lead Manager: IM&T Security & Resilience Manager
Conclusion of Equality Impact Assessment: There are no adverse effects of this policy on any group	
Recommendations for Action Plan: None	
Risks Identified: None	
Approved by a member of the executive team:	
YES	**NO**
Name: **Clare Chambers**	Position: **Head of IM&T**
Signature: **Approved via email**	Date: **4th February 2019**