NHS
East London
NHS Foundation Trust

Third Party Remote Access for IT Suppliers Policy

Version number :	1.2
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	20 February 2019
Name of originator/author:	Assistant Director of IT
Executive Director lead :	Chief Financial Officer
Implementation Date :	February 2019
Last Review Date	December 2018
Next Review date:	February 2022

Services	**Applicable**
Trustwide	x
Mental Health and LD	
Community Health Services	

CONTENTS

1.1 Introduction

In order to ensure that the Trust provides a secure and robust IT service, it is essential that 3rd Party access to key operational devices and/or systems is conducted through a robust framework that ensures that:

- Access is permitted through a mechanism that ensures appropriate controls are in place to restrict access to authorized 3rd Party organizations only;
- Any changes that are conducted are done so in accordance with the Trust Change Management procedures;
- There is a robust accountability framework present.

1.2 Equality and Diversity

The Trust is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy should be implemented with due regard to this commitment.

To ensure that the implementation of this policy does not have an adverse impact in response to the requirements of the Race Relations (Amendment Act), the Disability Discrimination Act 2005, and the Equality Act 2006 this policy has been screened for relevance during the policy development process and a full impact assessment conducted where necessary prior to consultation. The Trust will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

The Trust will endeavour to make reasonable adjustments to accommodate any employee/patient with particular equality and diversity requirements in implementing this policy and procedure. This may include accessibility of meeting/appointment venues, providing translation, arranging an interpreter to attend appointments/meetings, extending policy timeframes to enable translation to be undertaken, or assistance with formulating any written statements.

2.1 Objective

This document details the control mechanism for enabling remote access by a third party that requires legitimate access to any device. The implementation and maintenance of these controls will ensure that the Trust is able to:

· Manage Risk from Third Party Access;
· Ensure a secure Technical Environment through the control of access;
· Manage the connection life-cycle;
· Restrict access to authorized parties only;
· Limit liability.

3.1 Scope of policy

This document applies to all third party organizations that access the Trust infrastructure remotely.

4.1 Policy

4.2 Third party definitions

A third party is defined as any individual or organization that is not a Trust employee who requires access to any aspect of the Trust IT infrastructure for a specified purpose.

4.3 Network/Operational Device

Any item that forms part of the infrastructure of the Trust network, this includes servers, routers, firewalls and PC's. This list is intended as a representative sample and is not exhaustive.

4.4 Sensitive Data

Sensitive data is defined as either personal data, as defined by the Data Protection Act 1998, or Trust proprietary information.

4.5 Remote Access

For the purposes of this document, remote access is defined as any form of access obtained from an external location.

4.6 3rd Party Access Sessions – Internal session requests

All 3rd party access sessions must be made to the IT Infrastructure and Telecoms Development Manager (see contacts list at Appendix A) or in their absence a nominated member of their Team.

4.7 External Session Requests

In the event that a 3rd party access request is received, the request will be recorded by that member of the ICT Team and access granted for the duration of the approved session. All appropriate change management procedures must be adhered to. Appendix B is an example of a change management form.

4.8 Required Information

Whenever a request is made in relation to a remote access session, the following information must be recorded:

- Third Party (Organisation) Name
- Third Party Name (Designated Personnel) – person who will be connecting
- Contact details – phone and email
- Comprehensive Reason for Access
- RFC Details (If required)
- Date Access to be facilitated
- Details of Remote Access Session (Time/Date initiated, performed by, date session terminated etc.)

4.9 Authorised 3rd Party Organisations

Details of authorised 3rd Party organisations will be maintained by the Technical Support team and distributed to all relevant parties within the Trust.

4.10 Change Management

If the session is related to a change, as defined by the Change Management Policy, approval must be obtained from change management process.

4.11 Restriction of 3rd Party Access – authorised personnel

The third party will ensure that the authorised personnel are appropriately trained for providing the remote service.

4.12 Web Based Sessions

Each member of staff enabling a web based access session will have their own individual account in order to enable appropriate audit functionality. Accessing the web based solution via an account not belonging to the individual may result in disciplinary action.

4.13 N3 Sessions

It is accepted that there is a requirement for certain 3rd parties to access the Trust infrastructure via an N3 connection; these organisations are bound by the terms of this document.
Any remote access to the Trust infrastructure will be via the Trusts Remote Access System, a connection to the Trust network will then be established with all traffic passing through the Trust firewall.

4.14 Access Restrictions

Any Third Party access session MUST only occur when prior approval has been provided by the Trust. Unauthorised access may result in further action being taken against the third party in question.

4.15 Access Monitoring

Each remote access session must have a member of the appropriate Trust team monitoring the activity of the third party. In the event of the third party accessing sensitive data, a recording of the session will be maintained. Failure to comply with this requirement may result in disciplinary action.

4.16 Termination of Access

The Trust reserves the right to terminate any remote access session without prior notice. Access may also be terminated if an unauthorised session is detected. These sessions will be terminated as soon as it is established that there will be no adverse impact upon the system that is currently being accessed.

4.17 Outbound Communications

It is accepted that during a physical visit to the site, there may be a requirement for a third party to remotely connect to their organisations network whilst connected to a Trust device. Any such connection will be bound by the contents of this policy in a non-disclosure agreement (a copy of which is enclosed in Appendix C), and it is incumbent upon the third party that there is adequate security architecture in place.

4.18 Audit Lifecycle

All remote access sessions will be subject to a full and comprehensive audit trail as per the Trust's Housekeeping and Monitoring Policy.

4.19 Reports

Reports will be produced on a regular basis in order to facilitate audit requirements. These reports will be stored for an appropriate period of time to ensure that they are available in the event of an incident. The reports will be reviewed monthly by the It and Telecoms Infrastructure Development Manager and Associate Director of IT and Systems Development.

4.20 Contractual Obligations

Any third party requiring remote access to Trust systems must sign and abide by the following document:

- Non-disclosure Agreement (Appendix C)

Failure to sign and comply with the requirements of these documents will prevent access from being obtained by the Third Party.

These documents may be substituted with other formal documents providing that they match the Trust's requirements. The Head of Information Governance should be consulted in those instances.

All agreements will be reviewed on a regular basis to ensure that they are both accurate and appropriate. A physical copy of the agreement will be retained by both the third party and the Trust.

5.1 Roles and Responsibilities

5.2 Trust Staff

It is the responsibility of Trust IT staff to ensure that this policy document is adhered to when enabling access for ANY third party individual or organisation.

5.3 Third Party Organisation

It is the responsibility of all third party organisations to:

- Abide by the controls detailed within this document;
- Sign and comply with the Non-Disclosure Agreement;

- To comply with the standards detailed within the Trust Information and Governance Security Policy and to ensure that a robust information security infrastructure is implemented and adhered to within their own organisation;
- To ensure that each access session is used solely for the agreed purpose for that connection.

6.1 Associated documentation and references

This document has been created in accordance with the following supporting documents:

- The Data Protection Act 1998
- The Computer Misuse Act 2000
- The Copyright, Designs and Patents Act 1988
- ISO 27001 The Code of Practice for Information Security Management
- Access is permitted through a mechanism that ensures appropriate controls are in place to restrict access to authorised 3rd Party organisations only;
- Any changes that are conducted are done so in accordance with the Trust Change Management procedures (Appendix B);
- There is a robust accountability framework present.

7.1 Training and resources

The IT team will ensure that there is a robust structure present, providing that the controls are in place to restrict third party access. The team has the technological capability to and will perform periodic reviews to ensure compliance with the requirements of this policy.

8.1 Monitoring and audit

This policy will be reviewed every 2 years or when there is significant change by the Information Governance Steering Group. Changes to the policy may also be made due to changes in legislation, technology or NHS guidance.

The Information Governance Steering Group monitors all Data Protection/Information Security policies, programmes and work plans, including compliance with this policy.

8.2 Recording and Monitoring of Equality & Diversity

The Trust understands the business case for equality and diversity and will make sure that this is translated into practice. Accordingly, all policies and procedures will be monitored to ensure their effectiveness. Monitoring information will be collated, analysed and published on an annual basis. The monitoring will cover all strands of equality legislation and will meet statutory employment duties under race, gender and disability. Where adverse impact is identified through the monitoring process the Trust will investigate and take corrective action to mitigate and prevent any negative impact.

The information collected for monitoring and reporting purposes will be treated as confidential and it will not be used for any other purpose.

APPENDIX A
ICT Contacts list

Asim Mir	Assistant Director of IT	020 7655 4092	Asim.Mir@nhs.net
John Morrison	Network Manager	020 7655 4093	John.Morrison1@nhs.net
Daniel Woodruffe	Chief Information Officer	020 7655 4083	Daniel.Woodruffe@nhs.net
Usman Malik	Server Team Manager	020 7655 4123	Usman.Malik2@nhs.net
John Smith	IT Project Manager	020 7655 4263	John.Smith39@nhs.net
Parm Basandrai	IT Project Manager	020 7655 4126	Parm.Basandrai@nhs.net
Kashif Ghafoor	IT Service Delivery Manager	020 3738 7203	K.Ghafoor@nhs.net

APPENDIX B – CHANGE MANAGEMENT FORM

Request Date	Click here to enter a date.
RFC Reference	Click here to enter text.

1. Service Details

System Name:

RFC Title: Click here to enter text.

2. Requester Details

Name: Click here to enter text.

Implementation Date: Click here to enter a date.

Stakeholders:

3. RFC Category

Standard ☐ **Emergency** ☐ **Other** ☐ **– Please Specify:** Click here to enter text.

4. Change Implementation Plan

Note: Please attach documentation/plan if too detailed for this section.

Testing Detail

Roll Back Plan

5. Reason For Change (Benefits/Business Justification)

6. Dependencies (e.g. Systems Directly Affected)

7. Risks/Issues Associated with Implementing The Change

8. Risks/Issues Associated with NOT Implementing The Change

9. Supporting Documentation

Yes ☐ **No** ☐

10. Other Comments

11. Submission Details

Any documentation to support this RFC should be attached to this document.

Please save in the format:
XXXX RFC Title *where XXXX is the RFC Reference*

This form should be saved in: SharePoint\IT Document Library\Change Controls\Changes for Review

PLEASE SEND THE COMPLETED FORM TO:
Change Control Panel (email distribution group)

APPENDIX C – Non-Disclosure Agreement
Confidentiality/Non-Disclosure Agreement for the Processing of Information for the East London NHS Foundation Trust Dated:
Parties:

(1) ELFT (Discloser)
(2) [Insert partner organisation name(s)]

Background

In consideration of the parties processing and disclosing confidential information to each other, they have each agreed to treat such information in accordance with and to otherwise abide by this agreement and the legislative requirements of the Data Protection Act 1998.

It is hereby agreed as follows:

1 **Interpretation**

1.1 "Confidential Information" means, subject as provided in Clause 3, all information of whatever nature (including without limitation business or technical information) in whatever form (tangible or intangible, human or machine readable or otherwise) obtained by either party (the "Recipient") directly or indirectly from the other party (the "Discloser") and whether or not such information (if in tangible form) is embodied in any materials or is classed as confidential or proprietary. Furthermore, Confidential Information is defined as Data as per the definition under the Data Protection Act 1998.

1.2 "Discloser" has the meaning given in Clause 1.1

1.3 "Materials" means documents, drawings, computer programs and other materials and physical items of any kind obtained from the Discloser and/or recording any Confidential Information including, without limitation, any of the same produced by or on behalf of the Recipient.

1.4 "Recipient" has the meaning given to it in Clause 1.1

2 **Confidentiality**

2.1 **No Use** – Recipient agrees not to use the Confidential Information in any way, or to manufacture or test any product embodying Confidential Information, except for the purpose defined within Section 9**.**

2.2 **No Disclosure** – The Recipient agrees to use appropriate controls to prevent and protect the Confidential Information, or any part thereof, from disclosure to any person or organisation other than the Recipients employees having a need for disclosure in connection with the Recipients authorised use of the Confidential Information.

2.3 **Protection of Secrecy** – The Recipient agrees to take all steps reasonably necessary to protect the secrecy of the Confidential Information, and to prevent the Confidential Information from falling into the public domain or into the possession of unauthorised persons. Furthermore, to prevent any person from unlawfully accessing or disclosing the data.

3 **Limits on Confidential Information**
Confidential Information shall not be deemed proprietary and the Recipient shall have no obligation with respect to such information where the information:

(a) was known to the Recipient prior to receiving any of the Confidential Information from the Discloser;
(b) has become publicly known through no wrongful act of the Recipient;
(c) was received by the Recipient without breach of this agreement from a third party without restriction as to the use and disclosure of the information;
(d) was independently developed by the Recipient without use of the Confidential Information; or
(e) was ordered to be publicly released by the requirement of a government agency.

4 **Ownership of Confidential Information**

The Recipient aggress that all Confidential Information shall remain the property of the Discloser, and that the Discloser may use such Confidential Information for any purpose without obligation to the Recipient. Nothing contained herein shall be construed as granting or implying any transfer of rights to the Recipient in the Confidential Information, or any patents or other intellectual property protecting or relating to the Confidential Information.

5 Breach

5.1 The breach by any of the persons referred to in Clause 2.2 of any of the obligations imposed on them as referred to in Clause 2.2 shall be deemed a breach of this Agreement by the Recipient.

5.2 The Recipient acknowledges that any breach by the Recipient of this agreement is likely to result in extensive loss and damage to the Discloser and that, as well as damages, an injunction would be an appropriate remedy for the Discloser in the event of such a breach.

5.3 If the Recipient becomes aware of any breach by the Recipient of this agreement the Recipient shall forthwith notify the Discloser in writing thereof, giving all available details, and shall at its own cost and at the Disclosers direction take such steps as the Discloser may decide in order to minimise the loss which the Discloser may otherwise suffer as a result of such a breach.

6 Destruction of Data

The Recipient agrees that once the purpose for receiving the Confidential Information is complete, that the Information shall be confidentially destroyed and a destruction certificate issued to the Discloser.

7 Survival of Rights and Obligations

This Agreement shall be binding upon, inure to the benefit of, and be enforceable by (a) the Discloser, its successors, and assigns; and (b) the Recipient and assigns.

8 Miscellaneous

8.1 No delay or failure by either party to exercise any right or remedy available to it under or in connection with this agreement shall prevent the later exercise of any such right or remedy.

8.2 Neither party shall sign this agreement without the prior written consent of the other , which shall not be unreasonably withheld.

8.3 This agreement does not create any partnership, agency or further relationship between the parties and does not oblige either party to negotiate or enter into any further contract with the other.

8.4 This agreement shall be governed and construed in accordance with English law and the parties hereby submit to the non-exclusive jurisdiction of the English courts.

9 Purpose of Agreement

[Insert precise purpose(s) of processing including any restrictions]