Essex Partnership University
NHS Foundation Trust

VIRTUAL PRIVATE NETWORK (VPN) REMOTE ACCESS POLICY

POLICY REFERENCE NUMBER	CP30
VERSION NUMBER	1.2
KEY CHANGES FROM PREVIOUS VERSION	Additional 3 months extension (GC Mar 21)
AUTHOR	Head of IT Service Delivery N & S
CONSULTATION GROUPS	North and South IT leads
IMPLEMENTATION DATE	October 2017
AMENDMENT DATE(S)	November 2018
LAST REVIEW DATE	N/A
NEXT REVIEW DATE	~~October 2020~~ ~~March~~ June 21
APPROVAL BY	Board of Directors
RATIFICATION BY	Not applicable
COPYRIGHT	

POLICY SUMMARY

The purpose of this policy is to set out clear guidelines to ensure that Virtual Private Network (VPN) access has the appropriate controls in place to protect the Trust, and its staff, against improper use whilst accessing the Trust's network remotely.

The Trust monitors the implementation of and compliance with this policy in the following ways;

Monitoring of implementation and compliance with this policy, and associated procedural guideline, will be undertaken by the compliance function and the Finance and Performance Committee as outlined in the associated procedural guideline.

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing the policy is Director of Information Technology and Telecommunication

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

VIRTUAL PRIVATE NETWORK (VPN) REMOTE ACCESS TO THE TRUST DATA NETWORK POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

VIRTUAL PRIVATE NETWORK (VPN) REMOTE ACCESS TO THE TRUST DATA NETWORK POLICY

This Policy document and the associated procedure sets out clear guidelines to ensure that the Virtual Private Network (VPN) access has the appropriate controls in place to protect the Trust, and its staff, against improper use whilst accessing the Trust's network remotely.

1.0 INTRODUCTION

1.1 This document forms the policy for VPN Remote Access to the Trust network. This policy will define standards for connecting and support, which are designed to minimise damage as a result of unauthorised access

2.0 SCOPE

2.1 This policy applies to all employees using a Trust owned computer or laptop used to connect to the Trust network.

2.2 This policy applies to remote access connections used to do work on behalf of Essex Partnership University NHS Foundation Trust (EPUT) including email, web resources, bespoke programs and network data.

2.3 This policy applies to implementations of VPN that are directed through the services provided and support by the Trust IT & Telecommunications Department which terminate the VPN.

3.0 POLICY PRINCIPLES

3.1 All applications, by staff, for VPN access must be made via the WorkSmart Portal, which can be access via the WorkSmart Portal link located on the Trust's Intranet.
https://servicedesk.eput.nhs.uk/RSDPortal/Workflow?workflowId=4&journeyId=44733&pageId=198

3.2 Only EPUT owned and procured equipment may be connected to the Trust network via VPN.

3.3 Remote PC's/Laptop's are an extension of the network, and as such are subject to the same rules, regulations and security policies that apply to on-site equipment.

3.4 General access to the Internet for recreational use by immediate household members, on connections provide by the Trust, will not be permitted. This may be subject to change in the future and this policy will be updated to reflect any such change and provide guidance on acceptable use.

3.5 Users shall directly access only those services that they are specifically authorised to use as defined by the Information Governance and Security Policy (CP50)

3.6 Access via VPN will be controlled by password and two factor authentication processes.

3.7 When actively connected to the corporate network via VPN, access will only be allowed to the Trust services that the user has access to when undertaking work for EPUT within a Trust premise.

3.8 Split Tunneling will not be permitted. As such any connection to a home network will be blocked and network printers on the home network will not be accessible.

3.9 All computers must have the most up-to-date anti-virus software, patches and service packs that are the corporate standard, and computers will be checked for compliance at every network connection attempt.

3.10 Only the EPUT approved Cisco or Microsoft IAG/UAG VPN clients may be used.

3.11 Any equipment that is to be used at a users' home will be preconfigured and tested prior to installation.

3.12 Hardware support is restricted to Trust property only. Any faulty equipment must be brought back to site for testing.

3.13 Software support is restricted to Trust property only.

3.14 IT & T support staff will make home visits only where absolutely required. All faulty equipment must be returned to work base.

4.0 ENFORCEMENT

4.1 Any user found to have violated this Policy, the Information Governance and Security Policy, Internet Access Policy, Email Policy and the Disciplinary Policy may be subject to loss of certain privileges or services.

5.0 GLOSSARY

5.1 Split-tunneling: Simultaneous direct access to a non-EPUT network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the Trust network via a VPN tunnel.

5.2 VPN: Virtual Private Network (VPN) is a method for accessing a remote network via secure "tunneling" through the Internet.

5.3 Split Tunneling: allows a VPN user to access a public network (e.g., the Internet) and a corporate network at the same time, using the same physical network connection.

5.4 Cisco VPN Client Software: A piece of software from Cisco Systems that creates the VPN connection from a user's laptop or PC to the corporate network.

5.5 Cisco SOHO VPN Router: A piece of hardware from Cisco Systems that connects to a broadband enabled phone line that creates the VPN connection from the hardware to the corporate network.

5.6 Microsoft IAG/UAG VPN Client Software: A piece of software from Microsoft Corporation that creates the VPN connection from a user's laptop or PC to the corporate network.

5.7 Two factor Authentication: The process of authentication an end user using two pieces of information, for example a Pin code and time restricted code.

END