Essex Partnership University
NHS Foundation Trust

Virtual Private Network (VPN) Remote Access Procedural Guidelines

POLICY REFERENCE NUMBER	CPG30
VERSION NUMBER	1.2
KEY CHANGES FROM PREVIOUS VERSION:	Additional 3 months extension (GC March 21)
AUTHOR	Head of IT Service Delivery N & S
CONSULTATION GROUPS	North and South IT leads
IMPLEMENTATION DATE	October 2017
AMENDMENT DATE(S)	N/A
LAST REVIEW DATE	N/A
NEXT REVIEW DATE	~~October 2020~~ ~~March~~ June 21
APPROVAL BY EXECUTIVE OPERATIONAL COMMITTEE:	October 2017
RATIFICATION BY FINANCE AND PERFORMANCE COMMITTEE:	October 2017
COPYRIGHT	© Essex Partnership University NHS Foundation Trust 2017-2021. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

POLICY SUMMARY

The purpose of these procedural guidelines is to provide the necessary information, to ensure that the appropriate access and controls are in place for staff whilst accessing the Trust's network remotely.

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

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing the policy is Executive Director of IT&T

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

VIRTUAL PRIVATE NETWORK (VPN) REMOTE ACCESS PROCEDURAL GUIDELINES

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 PROCEDURAL GUIDELINES

1.0 INTRODUCTION

These procedural guidelines aim to set out the Trust's rules relating to remote access, in order to ensure that the appropriate controls are in place to protect the Trust, and its staff, against improper use whilst accessing the Trust's network remotely.

2.0 SCOPE

2.1 All applications by staff in south Essex for VPN access must be made via the WorkSmart Portal, which can be accessed via the WorkSmart Portal link located on the Trust's Intranet. Applications for VPN access in North Essex are made via the equipment or software request link on the ICT services team page on IntraNEP.

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

2.3 Remote PCs/Laptops 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.

2.4 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 document will be updated to reflect any such change and provide guidance on acceptable use.

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

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

2.7 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.

2.8 Split Tunnelling 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.

2.9 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.

2.10 Only the EPUT approved Cisco VPN clients may be used.

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

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

2.13 Software support is restricted to Trust property only.

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

3.0 ENFORCEMENT

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

4.0 GLOSSARY

4.1 Split-tunnelling: 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.

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

4.3 Split Tunnelling: 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.

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

4.5 Cisco Home 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.

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

5.0 REFERENCES

END