



POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	Network Controls
Effective Date:	07 Jun 2019
Reference Number:	ISMS-09-01
Version Number:	1.0
Owner:	TRE Infrastructure and Security Management Process Owner,
Review Date:	07 Jun 2021

Table of Contents

1. Purpose	3
2. Scope	3
3. Responsibilities.....	3
4. Procedure.....	3
4.1. TRE Network Management.....	3
4.2. Communication Security.....	4
4.3. Network Service Levels	4
5. Cross-referenced ISMS Documents	5
6. Appendices.....	5

1. Purpose

Computer networks should be managed and controlled to protect information systems, applications and data. Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

This document defines the security mechanisms, service levels and management requirements of the network services used to support the TRE service.

2. Scope

All network services used by the TRE.

3. Responsibilities

There are no additional responsibilities specific to this guideline.

4. Procedure

4.1. TRE Network Management

Only authorised persons shall manage and maintain the operation of the TRE network.

The Centre for Health Informatics (CHI) is responsible for the management of the capital and revenue budget for the TRE network.

The TRE team has ownership of all network components comprising the TRE network and will oversee procurement of all network components that are to be connected directly or indirectly to the network.

The TRE team is responsible for the:

- Connection of any and all network components to the TRE network.
- Configuration and management of all network components comprising the TRE network.
- Management of all network based protocols (IP addresses, routing tables, DNS, DHCP, Routing protocols etc.).
- Management of all aspects of network security including authentication and control of access to the network.
- Performance monitoring.
- Disaster recovery of the network.
- Work with end users to support the resolution of problems as efficiently as possible.

The University of Manchester (UoM) IT Services is responsible for managing and maintaining the UoM network which is required for connectivity to the TRE. IT Services will provide network connectivity for users connecting from the UoM wired network.

Connections from outside of the UoM network will require use of the Janet network that is managed and maintained by the Joint Information Systems Committee (Jisc).

Users that are connecting to the TRE from non-academic institutions or academic institutions outside of the United Kingdom will be making use of additional networks that will be managed by additional organisations.

4.2. Communication Security

Cabling connecting to the UoM campus network is compliant with UoM cabling security.

There is a dedicated connection to NHS HSCN with cabling compliant to the NHS Code of Connection.

The TRE internal network is segregated into 3 zones: NHS NSCN, TRE internal and TRE demilitarised. The external network interfaces of each are protected by firewalls. Where possible white listing of IP address is used. Only the necessary ports required for operation are open. Only external facing network interfaces and only secure networking protocols are permitted, with the exception of DNS.

Perimeter defence firewalls protecting the TRE are ITSEC E3 and Common Criteria compliant.

Secure data transfers are permitted via SFTP over the public Internet, with the addition of SSH key pair exchange. All data transfers must have the appropriate agreement in place first and copies of the corresponding documentation will be stored within each TRE project's record.

The TRE has a dedicated NSCN node, which can only receive data transferred across NSCN via SFTP using SSH key pairs. The NSCN node cannot be bridged to any other network, not even the internal TRE network. However, there is a highly secure mechanism for transferring data between the NSCN node and the TRE that takes place within the TRE server room.

CHI has a secure office for data analysis that is located in Vaughan House with a private VLAN between workstations and servers. All network traffic across the VLAN is encrypted.

The topology of the TRE is available on request, at the discretion of the ISM.

Exclusions: UoM Phone systems, UoM campus network, UoM email system

4.3. Network Service Levels

All TRE users will gain connectivity through the UoM wired network. The service level agreement for this network is available from The UoM IT Services and is detailed online:

[UoM - Wired Network](#)

Users that are connecting from outside of the UoM network will gain connectivity through the JANET network. The service level agreement for this network is detailed here:

[Jisc- Janet IP connection](#)

Users that are connecting from the NHS will be making use of the HSCN network. The TRE uses British Telecommunications for connectivity to this network.

Users that are connecting to the TRE from non-academic institutions or academic institutions outside of the United Kingdom will be making use of additional networks that will be managed with different service level agreements.

5. Cross-referenced ISMS Documents

Number	Type	Title
<NO DATA>	<NO DATA>	<NO DATA>

6. Appendices

None