POL008 IT Network & Infrastructure Policy

Version	**1.1**
Ratified By	Integrated Governance Board
Date Ratified	June 2018
Date of Issue via Intranet	August 2018
Date of Review	**June 2019**
Lead Officer	**Ian Hart**
Executive Lead	**Debbie Bywater**

Contents

Information Reader Box	
Directorate	
Communications & Engagement	Information Technology
Continuing Healthcare	Corporate Affairs
Contract Management	Business Intelligence
Finance	Human Resources
Publications Gateway Reference	xx
Document Purpose	Policy and High Level Procedures
Document Name	IT Network & Infrastructure Policy
Author	Information Technology
Publication Date	June 2017
Target Audience	All CSU Employees
Additional Circulation List	n/a
Description	Policy for defining use of the Network Infrastructure and File Servers
Cross Reference	n/a
Superseded Document	n/a
Action Required	To Note
Timing/Deadlines	n/a
Contact Details (for further information)	Ian Hart, Assistant CIO 1829 Building Countess of Chester Health Park Liverpool Road Chester CH2 1UL Ian.Hart@nhs.net 01244 650546

-
Document Status
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

1 Introduction

This document defines the Network Infrastructure and File Server Security Policy for Midlands and Lancashire CSU

The Network Infrastructure and File Server Security Policy applies to all business functions and information contained on the network, file servers, the physical environment and to the relevant people who support the network.

This policy is intended to provide a high level summary of requirements for Midlands and Lancashire CSU and it should be noted that there a number of different infrastructures in use across MLCSU and that separate documented Operational Processes will be in place wherever relevant.

1.1 Purpose of Policy

- Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network infrastructure and file servers.
- Establishes the security responsibilities for network infrastructure and file server security.
- Provides reference to documentation relevant to this policy.

1.2 Scope of this Policy

This policy applies to all networks within Midlands and Lancashire CSU used for:

- The storage, sharing and transmission of non-clinical and clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images
- The provision of N3 networks allowing access to HSCIC systems

1.3 Aim of this Policy

The aim of this policy is to ensure the security of Midlands and Lancashire CSU. To do this the organisation will:

- Ensure Confidentiality
- Ensure Availability
- Ensure that the file servers are available for the users
- Protect the network from unauthorised or accidental access and modification by ensuring the accuracy and completeness of the organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.
- Protect the confidentiality, availability and integrity of the network by the development of business continuity and disaster recovery plans

2 Policy Statement

2.1 It is the policy of Midlands & Lancashire CSU that:

- The CSU information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality.

To satisfy this, the Midlands & Lancashire CSU will undertake to the following:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is appropriate with the risks to its network assets.
- Implement the Network & Infrastructure Policy in a consistent, timely and cost effective manner.

Where relevant, the Midlands & Lancashire CSU will comply with:

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 1998
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- The CCG will comply with other laws and legislation as appropriate.

2.2 Risk Assessment

Midlands & Lancashire CSU will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network infrastructure and file servers that are used to support those business processes. The risk assessment will identify appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability. Risk assessments will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the network.

Formal risk assessments will be undertaken and conform to ISO17799.

2.3 Physical and Environmental Security

Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers, entry and alarm controls.

The CSUs IT Managers accountable for Technical Services are responsible for ensuring that door lock codes are changed periodically or following a compromise of the code, if they suspect the code has been compromised.

- Critical or sensitive network equipment will be protected from power supply failures.
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to secure data centre areas must be authorised by the relevant CSU IT Manager accountable for Technical Services. All visitors to data centre areas must be made aware of network security requirements.
- All visitors must provide 2 forms of ID as additional assurance.

A log to all secure data centres must be maintained. The log will contain name, organisation, purpose of visit, date, and time in and out of all none Midlands & Lancashire CSU

All visitors to network cabinet areas must be authorised by the relevant CSU IT Manager accountable for Technical Services.

The CSU IT Managers accountable for Technical Services in each region will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted when necessary.

2.4 Access Control to Secure Network Areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The CSU IT Managers accountable for Technical Services in each region, will maintain and periodically review a list of those with unsupervised access.

Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- There must be a formal, documented user registration and de-registration procedure for access to the network.
- Departmental managers must approve user access.
- Access rights to the network will be allocated on the requirements of the user's job, rather than status.

- Security privileges (i.e. 'superuser' or network administrator rights) to the network controls will only be granted by the CSU IT Managers accountable for Technical Services in each region
- All users to the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities Policy)
- User access rights will be immediately removed or reviewed for those users who have left the CSU, changed jobs or have been suspended.

2.5 Third Party Access Control to the Network

Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.

- All third party access to the network must be logged.
- All third party access must be governed by NHS standards on Confidentiality and Data Protection.
- No third party can be connected unless the CSU IT Manager accountable for Technical Services in the relevant region is satisfied that the NHS standards on Confidentiality and Data Protection have been included in the third party contract.
- Access levels for third parties will only be granted to the level required for the third parties work.
- Third party access will never be allowed Root or similar administrative rights. The third party will have their own separate account.

2.6 External Network Connections

Ensure that all connections to external networks and systems have documented and approved System Security Policies.

- Ensure that all connections to external networks and systems conform to the NHS-wide Network and File Server Security Policy, HSCIC Statement of Compliance and supporting guidance.
- Designated Home Workers can only connect to the network via Midlands & Lancashire CSU standards and network equipment.

Maintenance Contracts

Midlands & Lancashire CSU IT Dept will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Midlands & Lancashire CSU IT Asset register.

2.7 Data and Software Exchange

Formal agreements for the exchange of data and software between organisations must be established and approved by the Information Governance Manager through an Information Sharing Protocol.

2.8 Fault Logging

The CSU IT Managers accountable for Technical Services in the each region are responsible for ensuring that a log of all server faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

2.9 Data Backup and Restoration

The CSU IT Managers accountable for Technical Services in the each region are responsible for ensuring that backup copies of file server data are taken regularly and for backing up the network devices configuration files.

- Documented procedures for the backup process, verification and storage of backup tapes will be produced and communicated to all relevant staff.
- All backup tapes will be stored securely and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- Users are responsible for ensuring that they backup their own data to the network server.

2.10 User Responsibilities

Midlands & Lancashire CSU IT Dept. will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

- All users of the network must be made aware of the contents and implications of the IT Network & Infrastructure Policy
- Irresponsible or improper actions by users may result in disciplinary action(s).
- Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.
- Users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time.
- All workstations will have a password activated if a workstation is left unattended for a short time.
- Users failing to comply will be subject to disciplinary action.

2.11 Malicious Software

The CSU IT Managers accountable for Technical Services in the each region must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

Internet
The CSU IT Managers accountable for Technical Services in the each region must ensure that appropriate measures are in place to monitor Internet traffic and activity.

2.12 Secure Disposal or Re-Use of Equipment

Ensure that where equipment is being disposed of, IT Service Delivery staff must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible IT Service Delivery staff should physically destroy the disk or tape.

Ensure that where disks are to be removed from the premises for repair, where possible, the data is securely overwritten or the equipment de-gaussed by the IT Service Delivery Team.
Where equipment is to be disposed of a certification of disposal must be supplied by the disposal company.

2.13 Change Control

Ensure that the CSU IT Managers accountable for Technical Services in the each region review changes to the security of the network infrastructure.
They must also ensure that they:

- Review changes to the security of the network servers.
- Review all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures are updated
- Adhere to the Change Management Policy

2.14 Security Monitoring

Ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

2.15 Reporting Security Incidents

All potential security breaches, incidents and weaknesses must be reported to Information Security Team.

2.16 Business Continuity Plans

The CSU IT Managers accountable for Technical Services in the each region ensure that business continuity plans and disaster recovery plans are produced for the file servers and Network infrastructure services defined in the CSU Principle Systems and Assets Registers.

3 Scope

3.1 Officers Within the Scope of this Document

3.1.1 Officers of the following Midlands & Lancashire CSU areas are within the scope of this document:

- All areas

3.2 Officers Not Covered by this Document

3.2.1 There are no Officers of Midlands & Lancashire CSU (Information Technology) not covered by this document.

4 Roles & Responsibilities

4.1 Sub-heading on contents page

4.2 Sub-heading not on contents or paragraph text

5 Corporate Level Procedures

5.1 Sub-heading on contents page

5.2 Sub-heading not on contents or paragraph text

6 Distribution & Implementation

6.1 Distribution Plan

6.1.1 This document will be made available to all Officers via the Midlands & Lancashire CSU internet site.

6.1.2 A global notice will be sent to all Officers notifying them of the release of this document.

6.2 Training Plan

6.2.1 A training needs analysis will be undertaken with Officers affected by this document.

6.2.2 Based on the findings of that analysis appropriate training will be provided to Officers as necessary.

6.2.3 Guidance will be provided on the intranet site.

7 Monitoring

7.1 Compliance

7.1.1 Compliance with the policies and procedures laid down in this document will be monitored via the IT Strategy Board together with independent reviews by both Internal and External Audit on a periodic basis.

7.1.2 Debbie Bywater, in conjunction with the Chris Knight, is responsible for the monitoring, revision and updating of this document.

7.2 Equality Impact Assessment

7.2.1 This document forms part of Midlands & Lancashire CSU's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

7.2.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

8 Associated Documentation

8.1 IT_001 IT Asset Management Policy

8.2 IT_002 User Account Management Policy

8.3 IT_004 IT Business Continuity Policy

9 References

n/a

Appendix 1 Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
0.1	01/06/2017	Ian Hart	DRAFT	
1.0	15/06/2017	Ian Hart	Approved	Approved by IT Architecture Board
1.0	11/12/2017	Ian Hart	RATIFIED	Integrated Governance Board

Appendix 2 Definitions

Unless a contrary intention is evident or the context requires otherwise, words or expressions contained in this document shall have the same meaning as set out in the National Health Service Act 2006 and the Health & Social Care Act 2012 or in any secondary legislation made under the National Health Service Act 2006 and the Health & Social Care Act 2012 and the following defined terms shall have the specific meanings given to them below:

CSU Executive	means the Managing Director and Executive Members collectively as a body.
Budget	means a resource, expressed in financial terms, proposed by the CSU Executive for the purpose of carrying out, for a specific period, any or all of the functions of the CSU.
Clinical Commissioning Group/CCG	means a body established in accordance with section 1I of the NHS Act 2006.
Employee	means a person paid via the payroll of Midlands & Lancashire CSU.