Policy Reference – POL008

Wirral Clinical Commissioning Group

ICT NETWORK AND INFRASTRUCTURE FILE SERVER POLICY

Version	**1.0**
Ratified By	**CCG Committee which includes Information Governance in the Terms of Reference**
Date Ratified	**5th March 2013**
Author(s)	**Ian Hart, Chief Operating Officer, Cheshire ICT Service**
Responsible Committee / Officers	**CCG Committee which includes Information Governance in the Terms of Reference**
Issue Date	**5th March 2013**
Review Date	**12 months from date of issue**
Intended Audience	**All CCG Employees**
Impact Assessed	**Yes**

Policy Reference – POL008

This policy covers the following organisations:

- NHS West Cheshire Clinical Commissioning Group
- NHS Eastern Cheshire Clinical Commissioning Group
- NHS Warrington Clinical Commissioning Group
- NHS Vale Royal Clinical Commissioning Group
- NHS South Cheshire Clinical Commissioning Group
- NHS Wirral Clinical Commissioning Group

Further information about this document:

Document name	**Cheshire ICT Service Network Infrastructure File Server Policy**
Category of Document in The Policy Schedule	**Corporate**
Contact(s) for further information about this document	**Mark Bakewell** **Chief Finance Officer**
This document should be read in conjunction with	**All other Cheshire ICT Service policies**
Published by	**NHS Wirral Clinical Commissioning Group supported by Cheshire ICT Service** **Clark House** **Hurdesfield Industrial Estate** **Hulley Road** **Macclesfield** **SK10 2LU**
Copies of this document are available from	Website: www.wirralccg.nhs.uk/About%20Us/ourpolicies.htm or NHS Wirral Clinical Commissioning Group, Old Market House, Hamilton Street, Birkenhead, Wirral, CH41 5AL

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0		

Policy Reference – POL008

1.0 Introduction

This document defines the Network Infrastructure and File Server Security Policy for Clinical Commissioning Groups (CCGs)

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.

2.0 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.

3.0 Scope of this Policy

This policy applies to all networks within Clinical Commissioning Groups 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 the Connecting for Health Programme
- The principle assets covered by this policy can be found in each CCG Principle Systems and Assets Register

4.0 Aim

The aim of this policy is to ensure the security of Clinical Commissioning Group's networks. To do this the CCG will:

- Ensure Confidentiality
- Ensure Availability
- Ensure that the network is for users.
- Ensure that the file servers are available for the users
- Preserve Integrity
- 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.

5.0 The Policy

The overall Network infrastructure and File Server Security Policy for THE Clinical Commissioning Groups is described below:

The CCG 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 CCG 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 commensurate with the risks to its network assets.
- Implement the Network infrastructure and File Server Security Policy in a consistent, timely and cost effective manner.

Where relevant, the CCG 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.
The policy forms part of the ICT Security policy and reflects the objectives of the Information Security Management System (ISMS).

6.0 Risk Assessment

The CCG 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 the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Risk assessment 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.

7.0 Physical & 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 ICT Technical Team Leader is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised, or when required to do so by the ICT Security Service.
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 ICT Technical Team Leader
- All visitors to data centre areas must be made aware of network security requirements.
- 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 Cheshire ICT Service staff
- All visitors to network cabinet areas must be authorised by the ICT Technical team leader.

The ICT Technical Team Leader will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted when necessary.

8.0 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 ICT Technical Team Leader 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.
- Remote access to the network will conform to the CCG Laptop and Portable Devices and Remote Access Policy.
- 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 Technical Services Manager.
- 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 CCG, changed jobs or have been suspended.

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 ICT Area Manager 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.

9.0 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, Connecting for Health Statement of Compliance and supporting guidance.
- The ICT Security Service must approve all connections to external networks and systems before they commence operation.
- Designated Home Workers can only connect to the network via Cheshire ICT Service standards and network equipment.

Maintenance Contracts
The Cheshire ICT Service will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Cheshire ICT Service Asset register.

10.0 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.

11.0 Fault Logging

The ICT Technical Team Leader is 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.

The ICT Area Manager is responsible for ensuring that a log of all networking equipment is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

12.0 Security Operating Procedures (SyOps)

Produce Security Operating Procedures (SyOps) and security contingency plans that reflect the Network and File Server Security Policy.
Changes to operating procedures must be authorised by the ICT Security Service

13.0 Network Operating Procedures

Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation.
Changes to operating procedures must be authorised by the ICT Security Service

14.0 Data Backup and Restoration

The ICT Technical Team Leader is 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.

15.0 User Responsibilities, Awareness & Training

The Cheshire ICT Service 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 Network and File Server Security Policy, Confidentiality, Data Protection and Health Care Records Policies
- Irresponsible or improper actions by users may result in disciplinary action(s).

16.0 Security Audits

The ICT Security Service will require checks on, or an audit of, actual implementations based on approved security policies.

17.0 Malicious Software

The ICT Technical Team Leader must ensure that measures are in place to detect and protect the network from viruses and other malicious software.

Internet
The ICT Area Manager must ensure that appropriate measures are in place to monitor Internet traffic and activity.

Email
The ICT Area Manager must ensure that appropriate measures are in place to monitor Email traffic and activity

18.0 Secure Disposal or Re-use of Equipment

Ensure that where equipment is being disposed of, ICT 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 ICT 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 ICT Service Delivery Team.

Where equipment is to be disposed of a certification of disposal must be supplied by the disposal company.

19.0 System Change Control

Ensure that the ICT Technical Lead reviews changes to the security of the network infrastructure.

Ensure that the ICT Technical Leader reviews changes to the security of the network servers.

All such changes must be reviewed and approved by the ICT Security Service.

- The ICT Area Manager is responsible for ensuring all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures are updated
- The ICT Security Service may require checks on, or an assessment of the actual implementation based on the proposed changes.
- The ICT Security Service is responsible for ensuring that selected hardware or software meets agreed security standards.
- As part of acceptance testing of all new network systems, the ICT Security Service will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

20.0 Security Monitoring

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

21.0 Reporting Security Incidents & Weaknesses

All potential security breaches must be reported to ICT Security Service.
All security incidents and weaknesses must be reported in accordance with the requirements of the Cheshire ICT Service incident reporting procedures.

22.0 Business Continuity & Disaster Recovery Plans

The ICT Area Manager must ensure that business continuity plans and disaster recovery plans are produced for the file servers and services defined in the CCG Principle Systems and Assets Registers

The ICT Area Manager must ensure that business continuity plans and disaster recovery plans are produced for the network infrastructure defined in the CCG Principle Systems and Assets Registers.

The plans must be reviewed by the ICT Security Service and tested on a regular basis.

23.0 Unattended Equipment and Clear Screen

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.

24.0 Security Responsibilities

The Cheshire ICT Service has delegated the overall security responsibility for security, policy and implementation to the ICT Security Service

25.0 Guidelines

Detailed advice on how to determine and implement an appropriate level of security is available from the ICT Security Service

26.0 Review

This policy will be reviewed 24 months from its date of approval. Earlier review may be required in response to exceptional circumstances or relevant changes in legislation.