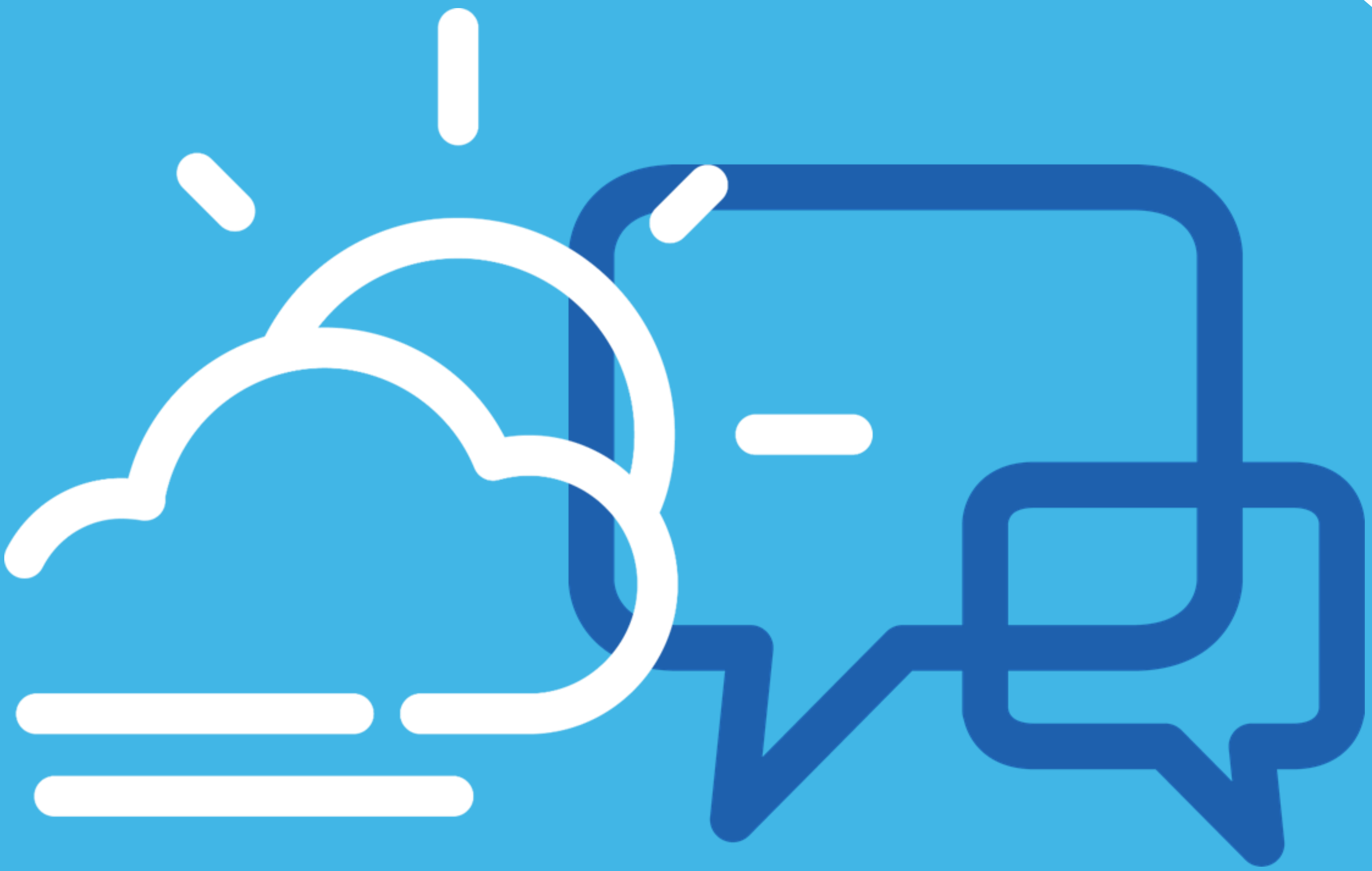
Network Security Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Network Security Policy**
Executive Summary:	The purpose of this document is ensure that the Trust IT Network is protected to a high standard in line with all the necessary legal frameworks and appropriate NHS policies and procedures, against potentially damaging threats, whether internal or external, deliberate or accidental.
Executive Lead:	Director of Finance and IM&T
Document Author:	Kevin Orritt, Infrastructure Manager
Document Purpose:	Policy
Target Audience:	All staff, contractors and third parties.
Additional Circulation List:	N/A
Date Ratified:	07/05/19
Ratified by:	Information Governance Steering Group
Consultation:	Via SharePoint
Cross Reference:	This document should be read in conjunction with related trust policies and procedures including all Information Governance Policies, and the Email and Internet Policy
Superseded Docs:	GMW Network Security Policy
Date of Equality Impact Assessment:	17/05/19
Board Objective Reference:	6 – to achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 17: Good governance
Risk Register Reference:	N/A
Contact Details for further information:	Andre de Araujo, Head of ICT
Document Status:	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.
Addendum:	27/08/19: IGSG approved addition of sections 4.22 Firewall Management & 4.23 Vulnerability & Patch Management and updates to section 4.17 in respect of logging.

Contents

1. Introduction 4
1.1 Purpose 4
1.2 Scope 4
2. Definitions 4
3. Duties 4
3.1 Board/Lead Committee 4
3.2 Director of Finance and IM&T 4
3.3 Employees 5
4. Processes and Procedures 5
4.1 Network Definition 5
4.2 Network Security 5
4.3 Physical and Environmental Security 6
4.4 Access Control to Secure Network Areas 6
4.5 Access Control to the Network 6
4.6 Third Party Access Control to the Network 6
4.7 Maintenance Contracts 7
4.8 Data and Software Exchange 7
4.9 Fault Logging and Rectification 7
4.10 Good Practice Guides 7
4.11 Network Operating Procedures 7
4.12 Data Backup and Restoration 7
4.13 Security Audits 8
4.14 Malicious Software 8
4.15 Secure Disposal or Re-Use of Equipment 8
4.16 System Change Control 8
4.17 Security Monitoring and Logging 8
4.18 Reporting Security Incidents & Weaknesses 9
4.19 System Configuration Management 9
4.20 Business Continuity & Disaster Recovery Plans 9
4.21 Unattended Equipment and Clear Screen 9
4.22 Firewall Management 9
4.23 Vulnerability and Patch Management 13
5. Training Requirements 15
6. Monitoring 15
7. Resource/Implementation Issues 15

8. Risk Issues 15
9. Requirements, Supporting Documents and References 16
9.1 Supporting Documents 16
9.2 References 16
10. Subject Expert and Feedback 16
11. Review 16
12. Appendices 16
Appendix 1 – List of Sites that form the Trust Network 17

1. Introduction

1.1 Purpose

This document defines the Network Security Policy for Greater Manchester Mental Health NHS Trust (the Trust).

1.2 Scope

The Network Security Policy applies to all business functions and information contained on the Information Technology Network (the Network), the physical environment and relevant people who support and use the Network.

The scope of this policy is to ensure the security, protection of the confidentiality, integrity and availability of the Trust's network. To do this the Trust will:

- ensure availability;
- preserve integrity, protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets;
- preserve confidentiality;
- protect assets against unauthorised disclosure.

This policy applies to all Information Technology networks within the Trust used for:

- the storage, sharing and transmission of non-clinical data and images;
- the storage, sharing and transmission of 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.

2. Definitions

CREST - an accreditation and certification body that represents and supports the technical information security market, which is an approved accreditation body under the UK Government Cyber Essentials scheme. CREST certifies its member companies to provide Cyber Essentials services.

3. Duties

3.1 Board/Lead Committee

The Information Governance Steering Group is the accountable body for Network Security as delegated by the Trust Board.

3.2 Director of Finance and IM&T

The Director of Finance and IM&T is the accountable officer for the Trust. These duties are discharged through the Associate Director of IM&T.

3.3 Employees

All Trust members of staff have a general duty to act responsibly and professionally when dealing with the security of Trust information and resources. Within the scope of this policy, staff must be especially aware of the need to safeguard the information in their care on the Network and report any suspected or actual breaches in security to the Information Governance Manager who has a dual role as the Information Security Manager via the Trust's Datix system.

4. Processes and Procedures

4.1 Network Definition

The Trust's network is classified as the network infrastructure which is solely owned and managed by the Trust. It does not include those sites, users and devices which are managed by third parties under an SLA. Appendix 1 shows a list of sites that form the Trust network.

The network comprises of a collection of communications hardware such as servers, storage area networks, computers and another peripherals that are available to the user base.

4.2 Network Security

The Trust 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 Trust will undertake 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 nontechnical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.
- Where relevant, the Trust must comply with:
  - Copyright, Designs & Patents Act (1988)
  - Access to Health Records Act (1990)
  - Computer Misuse Act (1990)
  - The Data Protection Act (2018)
  - General Data Protection Regulation (2018)
  - 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 Trust will comply with other laws and legislation as appropriate.

4.3 Physical and Environmental Security

The Trust has an IM&T Server Room Access and Environmental Control Procedure available from IM&T that covers this section. Refer to this for further details and information on the physical and environmental security.

4.4 Access Control to Secure Network Areas

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job role requires it. Where practical and possible, all cabinets and associated areas will be secured and locked and periodically audited. The IT Infrastructure Manager is responsible for initiating such audits.

Those who require access to these areas will need to sign in and out the appropriate keys and entry devices to gain access.

4.5 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. This must conform to the Information Security Policy.

Remote access to the network will conform to the Trust’s Mobile Media Security Policy.

Access rights to the network will be allocated on the requirements of the user's job functions, rather than on a status basis.

Security privileges, (i.e. 'superuser' or network administrator rights), to the network will be allocated on the requirements of the user's job functions, rather than on a status basis.

User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs as detailed in the System Administration Policy.

Access control to core network components, e.g. switches, will be via named user accounts and passwords in accordance with Information Security Policy.

Wireless access to the corporate network is controlled using secure servers and user access is restricted by their active directory.

4.6 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.

Third party suppliers to the Trust and non-Trust devices are not allowed access to the Trust corporate network unless authorised by the Head of ICT. Any guest access facilities will be administered centrally by the IT Infrastructure team unless alternate arrangements are authorised by the IT Infrastructure Manager.

4.7 Maintenance Contracts

The Head of ICT will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

4.8 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.

4.9 Fault Logging and Rectification

IM&T Support Central is responsible for ensuring that a log of all faults on the network is maintained and assigned to the appropriate members of the ICT team.

The member of staff will then be responsible for rectifying the fault and closure with in the agreed SLA time scales.

4.10 Good Practice Guides

NHS Digital has produced Good Practice Guides to aid NHS organisations with network security related issues which can be accessed on their website https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/cyber-guides-and-policies/cyber-and-data-security-good-practice-guides. All operating procedures must fall within these guidelines.

4.11 Network Operating Procedures

Documented operating procedures must be prepared for the operation of the network, to ensure its correct and secure operation.

Changes to operating procedures must be authorised by the IT Infrastructure Manager.

4.12 Data Backup and Restoration

The IT Infrastructure Manager is responsible for ensuring that backup copies of network configuration data are taken regularly, that all system databases and user data are backed up and checked regularly.

Backups will be regularly tested for errors and system databases will be restored and tested for consistency on a monthly basis.

Documented procedures for the backup process and storage of backup files will be produced and communicated to all relevant staff.

4.13 Security Audits

The Trust will require checks on, or an audit of, actual implementations based on approved security policies. This will be performed as part of the requirements of the NHS Digital Data Security and Protection Toolkit. Both internal and external assurance must be sought.

Penetration testing will take place at least once annually as per the Data Security & Protection (DS&P) toolkit standards. This will be done by the Trust's preferred security partner who must be CREST registered.

4.14 Malicious Software

The Trust will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

4.15 Secure Disposal or Re-Use of Equipment

Network equipment falls into the category of IT equipment and must be disposed of as per the Trust's Waste Management Policy and Procedures.

4.16 System Change Control

All changes to the network must be documented and agreed. All such changes must be reviewed and approved by the IT Infrastructure Manager. The IT Infrastructure Manager is also responsible for updating all relevant design documentation and operating procedures.

The International Standards Organisation (ISO) may require checks on, or an assessment of the actual implementation based on the proposed changes.

The IT Infrastructure Manager is responsible for ensuring that selected hardware or software meets agreed security standards.

Acceptance testing schedules for all new network systems must take place prior to any changes to the technology used for security of the network.

Testing facilities will be used for all new network systems. Development and operational facilities will be separated.

4.17 Security Monitoring and Logging

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

The IT Infrastructure Manager is responsible for ensuring that monitoring is in place.

Logging from Network Systems, Applications and services can provide key information about service affecting events and cyber security incidents. System Log files will be managed and documented in a procedure with the following requirements.

- All key Network systems, (defined by Head of ICT), must enable logging.
- Logs must be retained for a minimum of 3 months.
- Logs must be securely stored with auditable access to restricted users in order to prevent tampering.
- Logs must be timestamped, with systems configured to use a reputable time source.
- Logs must be regularly backed up.
- Logs must be subject to regularly review and/or automated alerts to identify anomalies or malicious activity.

4.18 Reporting Security Incidents & Weaknesses

All potential security breaches must be investigated and reported to the IT Infrastructure Manager. Security incidents and weaknesses must be reported in accordance with the requirements of the Trust's Incident, Accident and Near Miss Policy.

4.19 System Configuration Management

The Trust must ensure that there is an effective configuration management system for the network. The IT Infrastructure Manager is responsible for this.

4.20 Business Continuity & Disaster Recovery Plans

The Trust must ensure that business continuity plans and disaster recovery plans are produced for the network. The plans must be held by the Head of IT and tested on a regular basis.

4.21 Unattended Equipment and Clear Screen

Users must ensure that they protect the network from unauthorised access. They must ensure that nobody can use their logon when they are away from their desk, the equipment is left unattended or they have finished working.

Users failing to comply will be subject to disciplinary action.

4.22 Firewall Management

The main aspects of firewall management are as follows:

- Firewalls should be used to separate the internal Trust network from all other networks outside of the Trusts direct control

- Firewall and router configurations must restrict connections between untrusted networks and any systems in the Trust network
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- Dedicated hardware should be used for firewall functions
- Firewall design should be Highly Available and resilient
- Firewall access should be tightly controlled, regularly reviewed and a principle of least privilege applied to access
- All changes to firewall configuration should be tightly change controlled
- Firewall configuration should be backed up on a regular basis
- Firewall policy should include provision for ensuring that default passwords are changed and strong passwords are implemented
- Firewall policy should include provision for ensuring that externally accessible services are disabled unless a documented business case exists and is approved after risk assessment
- Roles, groups and responsibilities must be documented for the management of network components
- Documentation must be created and maintained for use of all services, protocols and ports/services allowed
- A standard configuration should exist for a fast and consistent firewall deployment
- Physical access to the firewall must be restricted and efforts must be made to monitor and log the access to the firewall

The following sub-sections refer to specific requirements.

4.22.1 Firewall Capabilities

Hardware firewalls which include Stateful inspection technology must be implemented where the Trust network connects to eternal networks not within Trust control including the Internet and N3.

Firewalls must be fit for purpose and scalable for intended environments

4.22.2 Firewall Positioning

Perimeter firewalls must be positioned to enable them to act effectively as perimeter security devices and control inbound traffic to, and outbound traffic from the network.

The firewalls must be the first and only devices connected to all networks not under the direct control of the Trust. All other devices must be connected either directly or indirectly to the internal interface(s) of the firewalls.

Internal firewalls must be positioned to enable them to effectively control ingress and egress to the internal network areas they protect. There must be no network connection to each protected internal area other than through its firewalls.

4.22.3 Management Console Positioning

Firewall management consoles ideally should be located on the internal network in a separate VLAN to ensure segregation from normal network traffic. All management traffic is to be suitably encrypted.

4.22.4 Firewall Physical Location

Wherever possible the firewall and any management console must be installed in a physically secure location where access can be restricted to authorised personnel. Consoles should be and remain locked as a matter of course.

4.22.5 Access Control

All firewall administration consoles should be protected by username and complex password and with a second factor of authentication if this capability is available.

Default root/admin passwords must be changed to a suitable strong password prior to production commissioning.

If supported by the hardware, each person requiring administrative access should have their own credentials. If only shared access is possible, the required username and password must only be distributed amongst firewall administrators and must be changed whenever a firewall administrator leaves the organisation or moves to a role no longer requiring access.

The firewall console password must be changed at least every six months.

4.22.6 Rule base design

All rule base design should be based on an initial “Deny All” policy, whereby only traffic specifically permitted through the firewall in a rule is to be allowed.

All drop rules should be configured to drop packets rather than reject to protect against Denial of Service (DoS) attacks.

All allow rules must have a Source, Destination and Service (port) defined. Rules containing “Any” as a source or destination in are only permitted in Deny rules, however in special circumstances may be included in an Allow rule if approved by change control following a risk-assessment

4.22.7 Rule order

Rules are to follow the following order:

1. Traffic allowed directly to the firewall (e.g. Management Traffic).

2. The second set of rules should block any other traffic to the firewall itself
3. Allowed traffic originating from the firewall. (e.g. External Logging).
4. The fourth set of rules should block any other traffic from the firewall.
5. Access rules that permit access to and from the trust network.
6. The sixth rule should be a drop all rule, i.e. any traffic that does not meet previous rules should be dropper (default-deny)

4.22.8 Additional Security Options

Anti-spoofing should be configured appropriately on all interfaces.

Stateful inspection of all traffic is to be enforced

4.22.9 Encryption

All Virtual Private Networks (VPN) must be implemented using Internet Protocol security (IPsec) with a minimum encryption algorithm of 3DES and hashing algorithm SHA-2.

Where possible, the more secure encryption algorithm AES 256 is to be used. The hashing algorithm MD5 is not to be used as it is less secure than SHA-2.

4.22.10 Network Address Translation (NAT)

NAT improves security by making the internal network invisible and non-routable from the outside world. At the same time however, NAT can introduce connectivity problems. A decision on whether NAT should be used must be made and documented prior to firewall deployment depending on the specifics of the site and network.

4.22.11 Demilitarised Zones (DMZ)

DMZs should be configured on all perimeter firewalls at the time of installation wherever possible.

All servers and systems that need to be accessed from the internet or networks external to GMMH should be placed in the DMZ.

4.22.12 Logs

GMMH will retain firewall logs as defined in section 4.17 of this policy.

4.22.13 Monitoring

GMMH should regularly review and develop a list of the types of traffic needed by the organization and how they must be secured including an analysis shall include which types of traffic can traverse a firewall under what circumstances

4.22.14 Backups

Firewall backup should be implemented in accordance with the standard GMMH backup policy.

Backup firewall configuration/rules must be taken prior to any configuration or rule changes being implemented, if a backup reflecting the current configuration has not already been taken.

Backups should also be taken following a successfully validated configuration or rule change.

4.22.15 Change Management

Changes to a rule base of a firewall that is already in place and live are permitted where required. When making changes to the firewall rule base the GMMH Change control policy should be followed. Firewall rule base changes must be signed off by a senior technician and the network manager or an infrastructure manager of equivalent or higher seniority.

For consistency, planning and risk management purposes, firewall rule base changes should be made during a planned change window. Only changes categorised as emergency changes and signed off by the Infrastructure Manager or equivalent or higher seniority may be made at any other time.

Change requests for rule changes should include ticket reference, description and reason for change, date and change owner details, in addition to any other information required as part of the standard change control process.

Change requests for rule changes should include details of relevant tests required to validate the rule change, and these should be completed following the implementation of the rule change and prior to signing off the change as complete.

All changes should include appropriate check to ensure current configuration has been backed up in accordance with the backup policy (see previous section).

4.23 Vulnerability and Patch Management

4.23.1 IT Infrastructure and associated components

GMMH shall comply with the minimum baseline requirements that are contained in this policy. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the GMMH assets and the data that resides on the system.

Any exception to this policy shall be documented and forwarded to GMMH Management for review and endorsement or rejection.

4.23.2 Applications

Any applications (both commercial-off-the-shelf and in-house) owned or managed by GMMH shall be updated with the necessary security patches. This is the default configuration for all applications.

Any exception to this policy shall be documented and forwarded to GMMH Management for review and endorsement or rejection.

System Owners are responsible for keeping their operating systems and applications updated and secure.

4.23.3 Enforcement

GMMH ICT staff and Internal Audit may without notice, conduct random assessments to ensure compliance with the principles of this policy.

Any system found in violation of this policy shall require immediate corrective action.

4.23.4 Exceptions

Exceptions to the GMMH Patching policy shall require formal documented approval from GMMH ICT Department.

Any servers, workstations or applications that do not comply with this policy shall have an approved exception on file with GMMH ICT Department.

4.23.5 Vulnerability Management

The deployment of any new infrastructure and/or applications, or the upgrade of existing infrastructure and/or applications that provide connectivity or services to environments external or internal to GMMH **should** be subject to a level of Vulnerability Assessment.

Vulnerability Assessments fall into two categories:

- Infrastructure Vulnerability Assessments.
- Application Vulnerability Assessments.

4.23.6 Timing

Sufficient time should be allocated within any project plan in order to allow the required scoping and organising of the Vulnerability Assessment.

Vulnerability Assessments for any infrastructure or application should be performed in as close to a ‘Live’ state as possible:

- Infrastructure Vulnerability Assessments **should** take place in the ‘To be Live’ environment just before ‘Go Live’, but with sufficient time to correct any major vulnerabilities.

- Application Vulnerability Assessments **should** take place in a test environment just before ‘Go Live’, but with sufficient time to correct any major vulnerability.
- Sufficient time should be allocated to enable mitigations and treatment activities to be completed before ‘Go Live’.

4.23.9 Reporting

Testers **shall** be instructed to report major vulnerabilities immediately.

Informal reporting on each day’s findings **should** be given to GMMH at the end of the day’s test.

The final test report **shall** be marked as ‘OFFICIAL – SENSITIVE’ and is to be in line with NCSC reporting guidelines.

5. Training Requirements

The Trust 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. This will be discussed at staff induction coursed and as part of on-going Information Governance training.

All users of the network must be made aware of the contents and implications of the Information Security Policy.

Irresponsible or improper actions by users may result in disciplinary action(s).

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Security incidents	Monthly	Datix incidents	Minutes	IT Infrastructure Manager	Risk Management

The Trust will monitor the effectiveness of the controls within this Policy through the use of Key Performance Indicators. These indicators will be regularly reviewed and submitted to the Information Governance Steering Group.

7. Resource/Implementation Issues

None identified.

8. Risk Issues

The Trust will carry out security risk assessments in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network 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 following the Trust's Risk Management Policy and will be the responsibility of the IT Infrastructure Manager.

9. Requirements, Supporting Documents and References

9.1 Supporting Documents

- IM&T Server Room Access and Environmental Control Procedure
- Information Security Policy
- Clinical System Access Policy
- System Administration Policy
- Mobile Media Security Policy
- Waste Management Policy and Procedures.

9.2 References

- Copyright, Designs & Patents Act (1988)
- Access to Health Records Act (1990)
- Computer Misuse Act (1990)
- The Data Protection Act (2018)
- General Data Protection Regulation (2018)
- 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)

10. Subject Expert and Feedback

Kevin Orritt – ICT Security Manager Kevin.Orritt@gmmh.nhs.uk
Andrea Cloke – Information Governance Manager Andrea.Cloke@gmmh.nhs.uk

11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.

12. Appendices

See following pages.

Appendix 1 – List of Sites that form the Trust Network

Site Name	Post Code	Current Supplier/Support Provider
Meadowbrook	M6 8HD	GMMH
Moorside Unit	M41 5SL	GMMH
Rivington Unit (RBH)	BL4 0JR	GMMH
Rockley House	M25 3JP	GMMH
Sungard	HX5 9DA	GMMH
Trust HQ Prestwich	M25 3BL	GMMH
Wentworth House	M30 9HF	GMMH
Woodlands	M28 0FE	GMMH
RBH Raid / Silverhill	BL4 0JR	Royal Bolton Hospital
April House	M1 2WR	GMMH
Arndale Chambers	BL1 1RJ	GMMH
Barrow SMS	LA14 1LU	GMMH
Beacon Centre	M6 6QT	Salford Council
Bentley & Barnett House	BL3 2RR	GMMH
Breightmet Health Centre	BL2 6NT	GMMH
Brook Heys	WA14 5JF	GMMH
Stocklund House	CA1 1PX	GMMH
Matrix House	PR6 0AA	GMMH
Acton Square	M5 4NY	GMMH
Cromwell House	M30 0GT	GMMH
Crossgate House	M33 7FT	GMMH
Chapel Road	M33 7EG	GMMH
Humphrey Booth Resource Centre	M27 5WW	Salford Council
Kendal SMS	LA9 4LT	GMMH
Kennedy House	WN7 2PJ	GMMH
Manor House	M41 9HE	GMMH
Orchard House Unit 11-12	M6 8FL	GMMH
Prescott House	M28 0ZA	GMMH

Site Name	Post Code	Current Supplier/Support Provider
St Wilfreds	PR1 2AS	GMMH
Ramsgate House/Bramley Street	M7 2YL	GMMH
Rico House	M25 9WS	GMMH
King Street	M30 0AE	Salford Council
Salford Probation	M6 6PF	GMMH
Westgate	WN8 8LP	GMMH
St James House	M6 5FW	GMMH
St Joseph Hostel	M30 8PF	GMMH
The Willows	M5 5JR	GMMH
Ashton Lane	M33 6WT	GMMH
Whitehaven SMS	CA28 7DG	GMMH
Wigan coops	WN1 1HR	GMMH
Wigan EDIT (upgrade)	WN7 4JY	GMMH
Workington SMS	CA14 2AY	GMMH
Trafford Raid - Wythenshaw	M23 9LT	UHSM
Chester Road, Trafford	M16 9HD	GMMH
Crisis Intervention/Liaison Salford Royal	M6 8HD	GMMH - Fibre link to Meadowbrook
Basement Aftercare Team	M30 0LH	Salford council
HMP Garth	PR26 8NE	Lancashire Care Trust
HMP Wymott	PR26 8LW	Lancashire Care Trust
HMP Preston	PR1 5AB	Lancashire Care Trust
HMP Haverrigg	LA18 4NA	Cumbria Partnership
Braeburn House (was Charles House)	M6 7DU	Priory
Lever Chambers	BL1 1SQ	GMMH
Anson	M14 5BY	GMMH
Oxford Rd - Chest Clinic (Bridges)	M13 9NL	GMMH
Chorlton	M21 9UN	GMMH
Clayton Health Centre	M11 4EJ	GMMH
Fallowfield Library	M14 7FB	GMMH

Site Name	Post Code	Current Supplier/Support Provider
Gaskell House	M13 0EU	GMMH
Hexagon Tower	M9 8GQ	GMMH
Kath Locke (Moss Lane East)	M15 5DD	GMMH
Kingslea	M20 4XP	GMMH
Laureate (Wythenshawe)	M23 9LT	GMMH
Longsight	M12 4LL	GMMH
Park House	M8 5RB	GMMH
Rusholme	M14 5NP	GMMH
Stables Primary	M20 2LR	GMMH
Station Road	M8 5EB	GMMH
Victoria Mill	M40 7LG	GMMH
Victoria Park	M40 5QN	GMMH
Withington	M20 2LR	GMMH
Cornbrook Quenby St (Ethnet)	M14 5RU	GMMH
Wythenshawe HC	M22 4PJ	GMMH
Silk Mill	M40 1HA	GMMH
Studio One	M22 0DW	GMMH
Bankley	M19 3PP	GMMH
Levenshulme	M19 3BX	GMMH
HMP Manchester	M60 9AH	GMMH
HMP Buckley Hall	OL12 9DP	GMMH
Ancoats Clinic	M4 6EE	GMMH
Baguley Health Centre	M23 1NA	GMMH
Brian Hore Unit	M20 2LR	GMMH
MaCartney House	M9 5XS	GMMH
Moss Side Health Centre	M14 4GP	GMMH
Rawnsley Building / Pearl Unit	M13 9WL	GMMH
Daisy Bank	M14 5QN	GMMH