Trust Policy

Network Security Policy

Issue Date	Review Date	Version
September 2017	**September 2022**	**4**

Purpose

This policy defines security and operational controls of ICT networks operated by Plymouth Hospitals IM&T Service.

Who should read this document?

All staff should familiarise themselves with this policy and its supporting policy documentation.

Key Messages

- Ensure the security of the networks operated by Plymouth Hospitals IM&T Service
- Ensure the availability of network infrastructure
- Preserve integrity of the network infrastructure
- Protect the network from unauthorised or accidental modification ensuring accuracy and completeness of the organisations assets.
- Preserve confidentiality
- Protect assets against unauthorised access and disclosure

Core accountabilities	
Owner	Jason Scott, ICT Security Coordinator
Review	Caldicott Information Governance Assurance Committee Technical IM&T Group
Ratification	Andy, Blofield, Chief Information Officer & Director of IM&T
Dissemination	Rob Harder, Head of IT Infrastructure
Compliance	Rob Harder, Head of IT Infrastructure

Links to other policies and procedures

Information Governance Management Framework
Information Security Policy
IM&T Change Management Policy
Third Party Network Access Form
Bring Your Own Device Policy

Version History

V1	March 2011	Initial Document
V2	March 2012	Revised and reformatted
V3.1	December 2012	Revised to include guidance on connecting devices once per month
V3.2	May 2013	Minor amendments to job titles
V3.3	August 2013	Minor amendments to password requirements
V3.4	March 2015	Review and minor amendments
V4	September 2017	Review and updated

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents on StaffNET. Larger text, Braille and Audio versions can be made available upon request.

Contents

1 Introduction

This document defines the Network Security policy for networks operated by Plymouth Hospitals IM&T Service. The Network Security policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

This document:

- Sets out the organisations policy for the protection of the confidentiality, integrity and availability of the network.
- Establishes the principles and responsibilities for network security.
- Provides reference to documentation relevant to this policy.

2 Purpose

The aim of this policy is to:

- Ensure the security of the networks operated by Plymouth Hospitals IM&T Service.
- Ensure availability of the networks
- Preserve integrity
- Protect Trust networks from unauthorised or accidental modification ensuring the accuracy and completeness of the organisations assets.
- Preserve confidentiality
- Protect assets against unauthorised access and disclosure.

3 Definitions

LAN	Local Area Network
WAN	Wide Area Network
SIRO	Senior Information Risk Owner
IM&T	Information Management & Technology
ICT	Information, Communication, Technology
HTTPS	Hypertext Transfer Protocol Secure
CMDB	Configuration Management Database
BYOD	Bring Your Own Device
ADF	Agile Desktop Framework
HSCN	Health and Social Care Network

4 Duties

Senior Information Risk Owner (SIRO)
The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board. The SIRO will also be the Director responsible for the Information Governance agenda. This role is undertaken by the Director of Corporate Business. The SIRO will delegate the day to day management of Information Governance to the Head of Clinical Systems Governance.

Senior IM&T Management Team
The senior IM&T management team are responsible for the delivery of ICT services and functions, reporting directly to the Director/CIO. The group is responsible for the review and ratification of this policy.

All Managers
Managers within the Trust are responsible for ensuring that the policy and its supporting standards are built into local processes and that there is ongoing compliance.

All Staff

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5 Main Body of Policy

The network is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information. The network utilises a variety of characteristics such as the medium used to transport data (e.g. copper or fibre), communications protocols such as HTTPS or Samba, scale (e.g. local area networks, wide area networks and wireless networks) and organisational scope.

The network must be able to withstand or recover from threats to its availability, integrity and confidentiality and, to satisfy this, Plymouth Hospitals IM&T Service provides the following assurance:

- To protect all hardware, software and information assets under its control. This is achieved by implementing a set of well-balanced technical and non-technical measures.
- To provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- To implement the Network Security Policy in a consistent, timely and cost effective manner.

Risk Assessments

Plymouth Hospitals IM&T Service undertakes security risk assessment(s) in relation to all the business processes covered by this policy which cover all aspects of the network that are used to support those business processes. The risk assessment identifies all the appropriate, cost effective security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Physical and Environmental Security

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

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

Critical network equipment is protected from power supply failures.

Critical network equipment is protected by intruder alarms or where this is not possible (e.g. plant rooms), the equipment is contained within secured cabinets with access restricted by existing building controls.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be authorised by the Technical Services Manager or authorised deputy.

Access Control

Entry to secure areas housing critical or sensitive network equipment is restricted to those whose job requires it.

Access to the network is via a secure log-on procedure. There is a documented and formal user registration and de-registration process for access to the network, held by Plymouth Hospitals IM&T Service.

Security privileges to the network are allocated on the requirements of the user’s job, rather than on a status or any other basis and this is configured within Active Directory or individual systems. Service accounts are restricted to log on to the servers or devices that they are applicable for.

All users to the network have their own individual username and password and sharing of credentials is strictly forbidden.

Users are responsible for ensuring their password is kept secret with password changes enforced on a 90 day rotation. Passwords must be a minimum of 8 characters, include an uppercase, lowercase and numerical character, not be any of the last three passwords nor contain the account name, first name or surname.

User access rights are removed or reviewed for those users who have left the Trust or changed jobs and user accounts are disabled automatically if not used in 100 days and deleted after a further 61 days. When the account is disabled and the user has a registered email address, the user is sent an email advising the account has been disabled.

Equipment

Only equipment approved by Plymouth Hospitals IM&T Service is permitted to connect to the network and all equipment is registered with the ICT Configuration Management Database (CMDB). No personal equipment is permitted for connection without explicit consent by Plymouth Hospitals IM&T Service and appropriate justification, with the exception of devices permitted under the BYOD (Bring Your Own Device) system.

Devices connected to the network are required to have up-to-date anti-virus and malware protection and where appropriate be centrally managed, updated, inventoried and audited. Plymouth Hospitals IM&T Service utilise Sophos Endpoint Protection, Microsoft SCCM, SNOW Software Asset Management and Active Directory group policies to perform these tasks and devices should be compatible with these products. Where specialist devices require network access and cannot accommodate these security controls they will be segregated from the Trust network using appropriate means.

Wireless Network

Access to the secure wireless network is restricted to authorised devices, controlled through Active Directory security group membership or static configuration policies on the wireless controllers. Access rights can be revoked centrally. User access is controlled through existing Active Directory policies.

Wireless transmissions are encrypted to WPA2 standards. Where devices do not support 802.1X authentication a shared key is utilised in conjunction with per-device network based access control, centrally enforced by the wireless management controllers.

Approved applications accessible on the wireless network are defined within the Telecommunications Policy.

Third Party Access

Third party access to the network, whether on-site or remotely, is based on a formal process which satisfies NHS security conditions. Third parties accessing systems that contain patient identifiable or confidential data require a valid IG Toolkit submission and satisfactory scoring.

Third party access to the network is restricted only to those devices or systems deemed necessary and appropriate and all such access to the network is logged for audit purposes.

Third party computers and laptops are required to have up-to-date anti-virus and malware protection installed. Mobile devices such as laptops must have encryption for data at rest.

By default, associated third party access is disabled and is enabled as and when required for a defined duration, on request through the Plymouth Hospitals IM&T Service.

Remote Access for NHS Staff

Access to email via NHSmail is possible from any Trust or personal device. Help and guidance is available on the NHSmail portal (www.nhs.net).

Remote access for Trust staff to business and clinical systems is available via the following methods:

- From Trust laptops using Aruba VIA software
- From personal devices, accessing the Agile Desktop Framework (ADF)

Staff do not need to apply for remote access when using Trust laptops and Aruba VIA. Staff wishing to use personal devices with ADF need to apply for access to ADF and request a two-factor authentication code (see below).

Remote access is provided for Trust-related activities only.

Two Factor Authentication

To access ADF from a personal device, the IM&T Service Desk need to provide the staff member with a two-factor authentication setup code. This should be used in conjunction with the Google or Microsoft Authenticator application, available from the applicable app stores.

Staff have a responsibility to secure Trust equipment when offsite and ensuring no other persons (i.e. family members) use the equipment.

Data Protection

Under no circumstances are staff permitted to download or store patient confidential information on personal devices.

Waivers

The Trust cannot be held liable for any loss or damage that may occur to personal data, programs or equipment through the use of these remote access facilities. Staff should ensure important personal data is appropriately backed up.

External Network Connections

All connections to external networks and systems must have documented and approved System Level Security Policies.

All connections to external networks and systems conform to the NHS-wide Network Security Policy, HSCN Connection Agreement and supporting guidance.

All connections to external networks are firewalled and where necessary include additional intrusion prevention measures.

The Technical Services Manager in conjunction with the IT Security Coordinator approve all connections to external networks and systems before they commence operation.

Maintenance Contracts

The Technical Services Manager ensures that maintenance contracts are maintained and periodically reviewed for all network equipment.

Fault Logging

Incidents and faults with the network are recorded within the IM&T business management system and the IM&T Service Desk.

Cyber Incident Procedures

Where a virus, malware, ransomware or other threat has been identified and verified, Plymouth Hospitals IM&T Service will liaise with the department concerned to isolate, resolve and re-enable the device on the network in a timely manner. During virus outbreaks the aim is to reduce the spread of infection to other systems and to minimise the impact on business functions.

Change Control

Changes to the network are conducted in accordance with the Plymouth Hospitals IM&T Service Change Control Policy.

Monitoring

Plymouth Hospitals IM&T Service ensures that the network and attached infrastructure are monitored for potential security breaches, failures and discrepancies utilising a mix of in-house and off the shelf monitoring devices and software. End user devices are, where possible, monitored via Sophos Endpoint Protection.

Audit logs for network access controlled through Active Directory are held for approximately 5 days.

Incidents will be reported on the Trust risk management system, Datix, and investigated accordingly.

System Configuration Management

Where supported, network infrastructure device configurations are automatically collected and archived by a central management system. Devices which are not managed by this system have their configurations archived manually on a monthly basis.

Personal computers and laptops should be connected to the network at least once per month to receive the latest updates and antivirus definitions.

Business Continuity

Business continuity procedures and guidance are covered under the Plymouth Hospitals IM&T Service Business Continuity Management plan, which includes information on disaster recovery.

Where cost effective and appropriate, resilience shall be built in to the infrastructure to mitigate the failure of any one component. Offline documentation will be available and kept up-to-date which will detail the procedures to undertake during disaster recovery situations.

6 Overall Responsibility for the Document

The CIO and Director of IM&T, using guidance from the senior IM&T management team, is responsible for ratifying this document. The ICT Security Coordinator has responsibility for the review of this document. The Head of ICT Infrastructure has responsibility for the dissemination and implementation of this document.

7 Consultation and Ratification

The design and process of review and revision of this policy will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and senior IM&T management team, ratified by the CIO and Directory of IM&T.

Non-significant amendments to this document may be made, under delegated authority from the Director of IM&T, by the nominated owner. These must be ratified by the Director of IM&T.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

8 Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document owner will be responsible for agreeing the training requirements associated with the newly ratified document with the named Director and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

9 Monitoring Compliance and Effectiveness

Compliance with this policy will be monitored by the completion of the Information Governance Toolkit submission process. The evidence submitted for submission is subject to annual audit.

Each requirement detailed in the Information Governance Toolkit has been assigned to a named expert lead. This role has the responsibility for assuring the SIRO on an annual basis that the evidence collected is of high quality, is relevant and up to date.

The Head of ICT Infrastructure, or delegated staff, will monitor national and local developments that may affect this policy.

Adherence to this policy takes place through business-as-usual activities across the technical services team within the IM&T department.

10 References and Associated Documentation

Key legislation and standards in respect of Network Security are:

- Where relevant, Plymouth Hospitals IM&T Service complies with:

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Data Protection Act 1998
- Electronic Communications Act 2000
- Freedom of Information Act 2000

Plymouth Hospitals IM&T Service complies with other laws and legislation as appropriate.

Dissemination Plan and Review Checklist — Appendix 1

Dissemination Plan	
Document Title	Network Security Policy
Date Finalised	September 2017
Previous Documents	
Action to retrieve old copies	To be managed by the Document Controller

Dissemination Plan			
Recipient(s)	**When**	**How**	**Responsibility**
All Trust staff	September 2017	Vital Signs	Information Governance Team

Review Checklist		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes

	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment — Appendix 2

Core Information	
Date	September 2017
Title	Network Security Policy
What are the aims, objectives & projected outcomes?	This policy defines security and operational controls of ICT networks operated by Plymouth Hospitals IM&T Service.

Scope of the assessment
This assessment will highlight any areas of inequality with the implementation of this policy.

Collecting data	
Race	This is mitigated as the policy can be made available in alternative languages.
Religion	The document has no impact in this area.
Disability	This is mitigated as the policy can be made available in alternative formats.
Sex	The document has no impact in this area.
Gender Identity	The document has no impact in this area.
Sexual Orientation	The document has no impact in this area.
Age	The document has no impact in this area.
Socio-Economic	The document has no impact in this area.
Human Rights	The document has no impact in this area.
What are the overall trends/patterns in the above data?	There are no trends/patterns in this data. External consideration has been given to Acts of Parliament, 2011/12 NHS Litigation Authority Risk Management Standards for NHS Trusts, Care Quality Commission Outcomes and Information Governance Toolkit requirements.
Specific issues and data gaps that may need to be addressed through consultation or further research	Trust wide documents can be made available in a number of different formats and languages if requested. No further research is required as there are no further equality issues.

Involving and consulting stakeholders	
Internal involvement and consultation	This policy has been compiled by the ICT Security Coordinator. The policy has been circulated for consultation to members of the IM&T service leads and senior management.
External involvement and consultation	External consideration has been give to Acts of Parliament, Information Governance Toolkit requirements and NHS Digital guidance.
Impact Assessment	
Overall assessment and analysis of the evidence	This assessment has shown that there could be an impact on race or disability groups. However, this document can be made available in other formats and languages if requested. The document does not have the potential to cause unlawful discrimination. The document does not have any negative impact.

Action Plan				
Action	Owner	Risks	Completion Date	Progress update
Provide document in alternative formats and languages if requested.	Head of IT Infrastructure	Potential cost impact.	Ongoing	This action will be addresses as and when the need occurs.