Walton Centre

Communications

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain	
07/01/2005	1.1	L wyatt	Update of technical information

Table of Contents

1. Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust.

The Trust acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Trust's Security Policy, Security Standards and Work Instructions Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line managers (in scope)
Compliance	All staff and contractors (in scope)
Monitoring	Information Security Officer Information Security Auditor

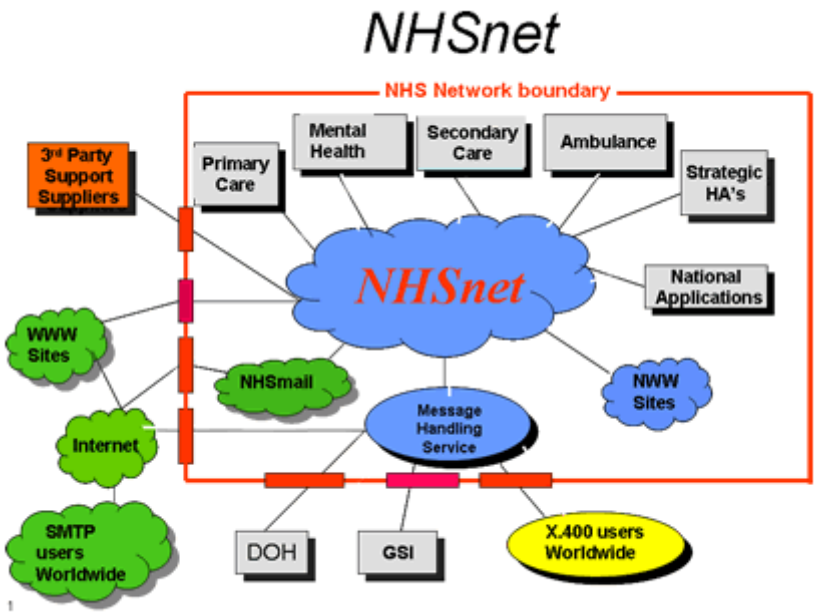
3. Network Protection

3.1 NHSnet

NHSnet consists of two managed network cores linking points-of-presence located in BT and Cable and Wireless premises. Individual sites connect by leased lines or dial-up connections to a point-of-presence. In the vast majority of cases, the service boundary of the network is a managed router on the customer premises. Each of the two wide-area network providers operates a core network linking their points of presence. The two network cores interconnect. Each network has a gateway to the Internet. On our behalf, the service providers operate managed Internet firewalls, managed firewall routers within GP practices and domain name services.

Both network providers operate customer helpdesks for ordering and fault resolution. The NHSIA also operates a helpdesk for fault escalation and general queries. Trust's, local Health Informatics Services and GP system suppliers are expected to provide first-line support services to GP practices, handling network-related issues on behalf of the practice. Syntegra, as operators of our Managed Message Handling Service (MMHS) email service also operate a helpdesk.

NHSnet is not an open network. Only certain organisations can connect. In connecting, NHS organisations make an undertaking to conform to some minimum standards of network and information security. These are intended to ensure that connecting organisations do not impose unnecessary security risks on the core network or on the other users of NHSnet. Staff members and contractors provided with access to NHSnet are expected to conform to the IT Security Policy of their host organisation and must be asked to agree to this as part of their contract of employment. The security standards for organisations connected to NHSnet include a requirement to implement adequate protection against email viruses and malicious software. The standards also require interconnections with untrusted networks to be managed in particular ways. These include a requirement for dial-up connections into NHS-connected networks to be protected by token-based strong authentication and a requirement for any TCP/IP connections to untrusted networks to be protected by a firewall accredited to ITSEC E3 or Common Criteria EAL4 Standard, using filtering rules approved by the NHSIA NHSnet Security Board.



NHSnet Schematic

3.2 Firewalls

3.2.1 Between the Trust and NHSnet

The Trust will put in place a firewall to protect itself from NHSnet and vice versa.

The chosen firewall product must be accredited to ITSEC E3 or Common Criteria EAL4.

3.2.2 Between the Trust and other external networks

It is mandated that NHSnet connected organisations with gateways to other external networks use a firewall product accredited to ITSEC E3 or Common Criteria EAL4. The firewall rules must be agreed with the NHSnet Security Board and must be subject to strict Change Control. NHSnet Security Managers must be contacted and agreement obtained before any changes are made.

3.2.3 Between the NHSnet and the internet (for information only)

The gateways to the Internet are to be provided and managed by the NHS Service Providers in accordance with defined rules agreed with the NHSnet Security Board. The firewall product must be accredited to ITSEC E3 or EAL4.

The secure Internet gateways must be able to:

- Prevent access to NHSnet from Internet based sources.
- Limit the types of sessions that NHSnet users can use through the gateway. This will minimise the risk of subversion of NHS host systems by non-NHS users and give the ability to restrict, monitor and/or evaluate any transactions or data passing across the boundary. This also limits the bandwidth loss caused by certain classes of session (e.g. Real Audio, Instant messaging applications).

The Trust may request changes to the Rule Tables of these firewalls to support its operational requirements. NHSIA change control forms should be emailed to both the Snr. NHSnet Security Manager for approval and possible subsequent action.

3.3 Intrusion Detection

The Trust will put in place appropriate intrusion detection systems and these will be monitored for inappropriate traffic / packets.

Logs will be kept for a minimum of twelve months and incidents will be dealt with in accordance with the Incident Reporting & Response Standards 12a, 12b and 12c as appropriate

4. Cabling

4.1 Leased Lines & LES circuits

4.1.1 Leased lines

Insert detail

4.1.2 LES circuits

Insert detail

4.2 Internal

The internal network is based on an ethernet configuration operating variously at 10/100mb and 1gb.

Network cabling consists of fibre optic backbones and category 5e cabling.

Where possible cabling has been built into the fabric of the buildings, utilising ducts and risers as protection. Where cabling cannot be protected within the fabric of the building it will be protected within trunking as far as desktop ports.

5. Wireless Communication

5.1 Bluetooth

Bluetooth is a short-range technology originally conceived for cable replacement by radio. A number of other uses have since been defined including LAN interconnect. Much effort has gone into producing low power, small and cheap Bluetooth modules to assist the take-up of the technology.

Bluetooth is an alternative to infra red connection technology; there is even an IR version of Bluetooth. IR requires strict clear line of site to operate, Bluetooth using radio can operate with obstructed line of site.

The primary characteristics of Bluetooth are:

- RF Power 1 to 100mW
- Frequency 2.4 to 2.4835 GHz
- Max number of communicating devices 8
- Max range 10 metres
- Frequency hopping at 1600 hops per second
- Maximum data throughput 1mbps (depends on application and level of encryption)

Authentication and encryption are included in the standard and both are at a higher level than used in 802.11b. 64-bit encryption is standard, with up to 128 bit available. Most Bluetooth devices currently available use the lowest possible RF power levels to limit range and enhance battery life. Because of the limited range and enhanced security features in the Bluetooth standard over 802.11b it is considered secure to use Bluetooth without any further security precautions.

5.2 802.11

5.2.1 802.11b with 40bit encryption as a minimum

Wireless networking to the IEEE 802.11 standards represents a low cost, easy of installation option for providing network connectivity. Unfortunately this easy of installation means that the Trust faces risks not only form the technology itself but also from unauthorised installation by well meaning, but technically unaware, users.

The 802.11b standards will allow for throughput of up to 11Mbps, providing a workable data flow. However, the needs to protect these data flows means that appropriate encryption is required which slows down the transmission to a rate which is not operationally satisfactory.

For this reason, the 802.11b standard will not be used by the Trust as part of its approach to network communications.

5.2.2 802.11g

The 802.11g standards will allow for throughput of up to 54Mbps, providing a workable data flow, even when appropriate encryption is applied.

For this reason the Trust will use only 802.11g wireless communications within its network.

To protect data flows and reduce the risks of illicit connection a range of countermeasures will be implemented including:-

Countermeasures to reduce the risk of eavesdropping	▪ Access Points will be sited so that they are not near windows or external walls. In the conflict between getting adequate coverage within a building and trying to minimise the external radiation the priority is to reduce the external signal. ▪ with the minimum power to provide the required coverage. ▪ Access points will not be connected to Ethernet hubs but to a LAN switch. ▪ If used externally, e.g. site to site with directional aerials and wireless routers/bridges, IPsec VPN and not WEP will be used.
Countermeasures to reduce the risk of illicit connection	▪ Shared key authentication as opposed to open null authentication is used. ▪ "Broadcast SSID" will be turned off on the Access Point. The default Broadcast SSID mode means the Access Point will accept any SSID. ▪ The SSID will not be the default

6. Remote Communication

6.1 NHSnet Based Terminal Services

The Trust provides access to network resources and applications to its users based at other NHS sites through the provision of terminal service access to the necessary servers.

Relevant ports on the Trust firewall will be opened to facilitate this service.

In order to access this service users must be connected to an NHSnet connected network and must provide their Trust user id and password in order to authenticate to the server.

The option to "shut down" will be removed from the available menu options for non-administrator users in order to prevent accidental shut down of the server.

6.2 Internet Virtual Private Network (VPN)

The Trust provides an internet based remote access solution in order to access its network when working off-site. In order to secure the transmission of data a VPN solution has been established which ensures that:-

VPN Gateway

- VPN Gateway functionality is a black box solution approved by the NHSIA and supplied by C&W. We limit activity via the IP range allocated to have only access to RDP and Citrix ports we do not manage the VPN Gateway or have access to any intrusion detection on the gateway.

Remote Client Machines

Where remote access to the Trust network is required:

- Remote client machines must be so configured that once a VPN session is established no other inbound or outbound network connection can be initiated outside the VPN tunnel.
- Remote client machines must have up to date Anti-Virus protection.

Where remote access to the Trust network is not required but access to applications hosted on the Trust network is required:

- Remote client devices other than those owned and managed by Organisations that have signed the NHSnet Code of Connection may be used providing that no data is written to any such client device.
- The client used must capable of supporting defined encryption levels.

- The VPN gateway is capable of defending the NHSnet connected infrastructure from attacks using malicious code.

6.3 3G / GPRS

6.3.1 NHSnet service provider managed solutions (for information)

The provision of 3G/GPRS services and the associated infrastructure is the responsibility of the NHSnet service provider. 3G/GPRS service solutions from NHSnet service providers must be proposed to and approved by the NHSnet Security Board.

6.3.2 Locally provided and managed solutions (other than via internet VPN)

The risks associated with the deployment of local 3G/GPRS services are high. Where such a solution is developed the following minimum security requirements will be applied:-

- The connection from the 3G/GPRS SAP to the Trust network will be protected by a firewall.
- The firewall protecting the Trust network will be a dedicated firewall in a two port configuration.
- The firewall protecting the Trust network must meet ITSEC E3/EAL 4 standard.
- The user accessing the Trust LAN from remote devices across an untrusted 3G/GPRS network must be authenticated by Strong Authentication.
- The 3G/GPRS SAP will be monitored and logs kept for a minimum of x months.

7. Compliance

7.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

7.2 Review and Monitoring

The Trust has in place routines to regularly audit compliance with this and other standards.