**USER NOTE: THIS IS AN EXAMPLE DOCUMENT ONLY; FINDINGS SHOULD REFLECT YOUR OWN ORGANISATION AND BS7799 REFERENCES SHOULD REFLECT BS7799-2:2002**

# 1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

| Name | Job Title | Signature | Date |
|---|---|---|---|
| Authored by:- <Name> | Information Security Consultant | | |
| Approved by:- <Name> | Information Security Officer | | |
| Authorised by:- <Name> | Director of Finance and IT | | |

# 2. Change History

| Version | Date | Author | Reason |
|---|---|---|---|
| Draft1.0 | | | 1st. Draft |
| Draft1.1 | | | 2nd. Draft include Appendices |
| Version 1.0 | | | 1st. Version also includes update to the residual risks to include homeworkers' access |
| Version 1.1 | | | 2nd. Version to include update to the list of assets |
| Version 1.2 | | | 3rd. Version to reflect changes to documentation references |
| Version 1.3 | | | 4th. Version – update to asset register |
| Version 1.4 | | | 5th. Version – update to reflect comments from Phase 1 audit |
| | | | |
| | | | |

# 3. Contents

# 4. Introduction

Potential losses arising from breaches of IT security include physical destruction or damage to the Trust's computer systems, loss of systems availability and the theft, disclosure or modification of proprietary information due to intentional or accidental unauthorised actions.

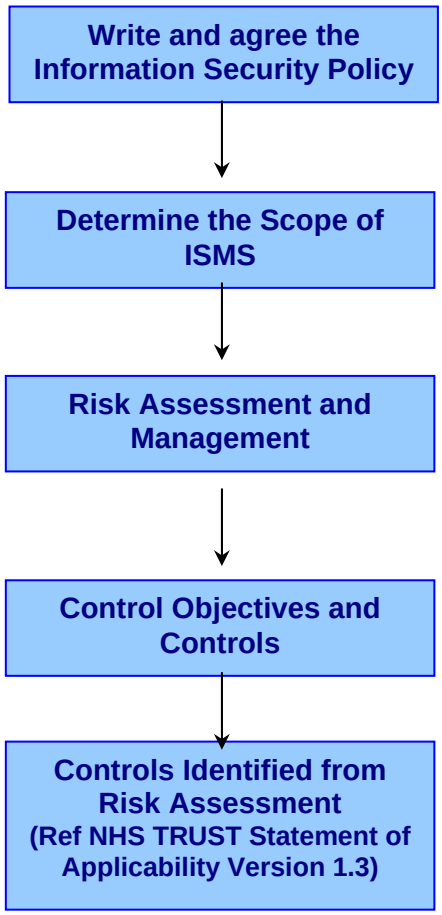
A wide spectrum of IT security threats have the potential to give rise to such losses. These range from accidental causes such as water damage and natural disaster to deliberate systems failure or damage caused by the malicious or criminal actions of individuals.

The potential business impact should such threats materialise also covers a wide spectrum. This ranges from tangible consequences such as specific operational or financial losses to intangible consequences such as loss of  public confidence, loss of ability to supply.

This document describes the risk assessment and management process adopted by the Trust and contains the results of the risk analysis which in turn determine the selection of control objectives and controls (see the NHS TRUST Statement of Applicability (SoA)).

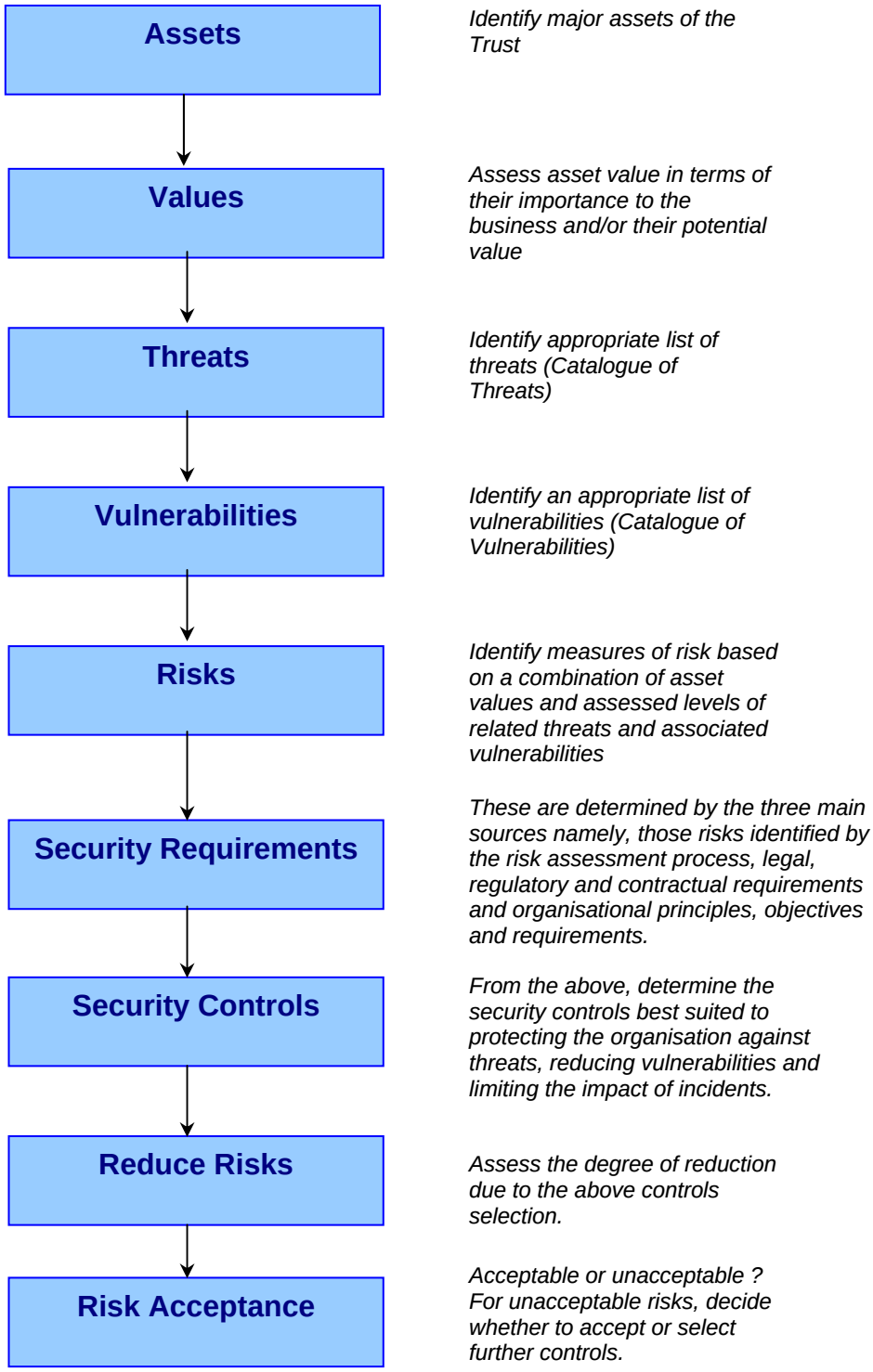
# 5. Overview of the ISMS Establishment Process

The following chart shows the various steps that have been undertaken by the Information Security team to establish the ISMS:



# 6. Overview of the Risk Assessment Process

The following chart shows the various steps that have been undertaken by the Trust's Information Security team during the risk assessment process:



# 7. Key Trust Information Assets

**EXAMPLE:**

| Trust Key Information Assets | Responsibility |
|---|---|
| People | HR |
| Computer Records (Electronic Information) | System Owners |
| Computer hardware | IT Operations |
| Computer Software | IT Operations |
| Networks (LAN/WAN) | IT Operations |
| Personnel, health and pension records | HR |
| Company financial records | Finance |
| Document Management | All |
| Intranet | IT Operations |
| QA Information Management | QA |
| Asset register | Finance |
| Trust Image and Reputation | Corporate & Communications |
| Services (heating, lighting, power etc.) | Site Services |

# 8. Inventory of Major Trust Information Assets

| Asset | Value (VH,H,M,L) | Threats (ref. Section 9) | Vulnerabilities (ref. Section 10) | Measure of Risk (Appendix B) |
|---|---|---|---|---|
| | | | | |
| **Paper Documents** | | | | |
| | | | | |
| Training Materials | M | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 3 |
| Personnel Files | VH | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 5 |
| Contracts | H | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 4 |
| Tax Returns | M | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 3 |
| Invoices and Utility bills | M | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 3 |
| Correspondence | M | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 3 |
| Bank Statements | L | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 2 |
| Financial Statements | L | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 2 |
| Emails | H | 1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28, | 4 |

| Asset | Value (VH,H,M,L) | Threats (see Section 9) | Vulnerabilities (see Section 10) | Measure of Risk (Appendix B) |
|---|---|---|---|---|
| **Physical Assets** | | | | |
| | | | | |
| Desktop PCs | L | 1.3, 1.7, 1.9, 1.13, 1.15, 1.16, 1.17, 1.20, 1.22, 1.24, 1.25, 1.27, 1.30, 1.34, 1.37, 1.41, 1.42, 1.43 | 2.2, 2.3, 2.4, 2.6, 2.10, 2.11, 2.15, 2.17, 2.18, 2.27, | 2 |
| Laptop PCs | L | 1.3, 1.7, 1.9, 1.13, 1.15, 1.16, 1.17, 1.20, 1.22, 1.24, 1.25, 1.27, 1.30, 1.34, 1.37, 1.41, 1.42, 1.43 | 2.2, 2.3, 2.4, 2.6, 2.10, 2.11, 2.15, 2.17, 2.18, 2.27, | 2 |
| Servers | M | 1.1, 1.2, 1.3, 1.4, 1.6, 1.7, 1.9, 1.10, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.20, 1.21, 1.22, 1.23, 1.24, 1.25, 1.27, 1.29, 1.30, 1.32, 1.34, 1.37, 1.38, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.16, 2.17, 2.18, 2.21, 2.29, 2.34, 2.35, 2.36, 2.38, 2.43 | 3 |
| Printers | L | 1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43 | 2.2, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.17, 2.18, 2.32, | 2 |
| Photocopiers | L | 1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43 | 2.2, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.17, 2.18, 2.32, | 2 |
| Telephones | L | 1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43 | 2.2, 2.7, 2.8, 2.9, 2.10, 2.11, 2.18, | 2 |
| Fax Machines | L | 1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43 | 2.2, 2.7, 2.8, 2.9, 2.10, 2.11, 2.18, | 2 |
| **Asset** | **Value (VH,H,M,L)** | **Threats (see Section 9)** | **Vulnerabilities (see Section 10)** | **Measure of Risk (Appendix B)** |

| | | | | |
|---|---|---|---|---|
| Network Hubs and Routers | VH | 1.1, 1.3, 1.4, 1.7, 1.9, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.28, 1.29, 1.30, 1.32, 1.34, 1.35, 1.36, 1.39, 1.43 | 2.3, 2.4, 2.6, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18, 2.25, 2.26, 2.34, | 5 |
| Backup Media | VH | 1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43 | 2.2, 2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.27, 2.28, 2.31, | 5 |
| Storage Cabinets | L | 1.3, 1.7, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.8, 2.9, 2.10, 2.11, 2.12, | 2 |
| General Office Equipment | L | 1.3, 1.7, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43 | 2.8, 2.9, 2.10, 2.11, 2.12, | 2 |
| | | | | |
| **Logical Assets** | | | | |
| | | | | |
| Applications software | L | 1.3, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.24, 1.25, 1.27, 1.28, 1.29, 1.32, 1.37, 1.38, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.5, 2.6, 2.12, 2.32, 2.33, 2.34, 2.37, 2.39, 2.40, 2.42 | 2 |
| Technical Software (eg. Windows) | L | 1.3, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.24, 1.25, 1.27, 1.28, 1.29, 1.32, 1.37, 1.38, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.5, 2.6, 2.12, 2.32, 2.33, 2.34, 2.37, 2.39, 2.40, 2.42 | 2 |
| **Asset** | **Value (VH,H,M,L)** | **Threats (see Section 9)** | **Vulnerabilities (see Section 10)** | **Measure of Risk (Appendix B)** |

| | | | | |
|---|---|---|---|---|
| Electronic Data | VH | 1.2, 1.3, 1.4, 1.9, 1.10, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.22, 1.23, 1.24, 1.25, 1.27, 1.28, 1.29, 1.30, 1.31, 1.32, 1.34, 1.37, 1.38, 1.39, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.28, 2.35, 2.38,2.43 | 5 |
| Networks | VH | 1.2, 1.3, 1.4, 1.9, 1.10, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.22, 1.23, 1.24, 1.25, 1.27, 1.28, 1.29, 1.30, 1.31, 1.32, 1.34, 1.37, 1.38, 1.39, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.28, 2.35, 2.38,2.43 | 5 |
| | | | | |
| **People** | VH | 1.1, 1.3, 1.7, 1.10, 1.14, 1.15, 1.16, 1.18, 1.21, 1.22, 1.27, 1.30, 1.33, 1.34, 1.43 | 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.11 | 5 |
| | | | | |
| **Services** | | | | |
| | | | | |
| Telephone System | H | 1.3, 1.5, 1.7, 1.8, 1.9, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.28, 1.30, 1.31, 1.32, 1.33, 1.34, 1.35, 1.36, 1.37, 1.39, 1.40, 1.41, 1.42, 1.43 | 2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18 | 4 |
| Heating/Air Conditioning | H | 1.1, 1.2, 1.3, 1.7, 1.9, 1.10, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.21, 1.22, 1.23, 1.27, 1.30, 1.33, 1.34,1.42, 1.43 | 2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18 | 4 |
| **Asset** | **Value (VH,H,M,L)** | **Threats (see Section 9)** | **Vulnerabilities (see Section 10)** | **Measure of Risk (Appendix B)** |

| | | | | |
|---|---|---|---|---|
| Electrical Supply | VH | 1.3, 1.7, 1.9, 1.13, 1.15, 1.16, 1.18, 1.22, 1.23, 1.30, 1.31, 1.42, 1.43 | 2.11, 2.17, 2.18, 2.25, 2.34 | 5 |
| Smoke/Gas detectors | VH | 1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.15, 1.18,1.22, 1.23, 1.30, 1.43 | 2.17, 2.18, 2.25, 2.34 | 5 |
| UPSs | H | 1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.15, 1.18,1.22, 1.23, 1.30, 1.43 | 2.3, 2.4, 2.6, 2.9, 2.10, 2.11, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18 | 4 |

| Asset | Value (VH,H,M,L) | Threats (see Section 9) | Vulnerabilities (see Section 10) | Measure of Risk (Appendix B) |
|---|---|---|---|---|
| Water Supply | M | 1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.14, 1.15, 1.16, 1.18,1.22, 1.23, 1.30, 1.43 | 2.44 | 3 |
| | | | | |
| **Trust Image and Reputation** | | | | |
| | | | | |
| Reputation with Suppliers | M | 1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27, 1.28, 1.30, 1.31, 1.33, 1.34, 1.36, 1.42, 1.43 | 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30, 2.35,2.43 | 3 |
| Reputation with Customers | VH | 1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27, 1.28, 1.30, 1.31, 1.33, 1.34, 1.36, 1.42, 1.43 | 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30, 2.35,2.43 | 5 |
| Public confidence | VH | 1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27, 1.28, 1.30, 1.31, 1.33, 1.34, 1.36, 1.42, 1.43 | 2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30, 2.35,2.43 | 5 |

# 9. Catalogue of Threats

| Ref. | Threat | Likelihood | Severity | Value | Ref. | Threat | Likelihood | Severity | Value |
|---|---|---|---|---|---|---|---|---|---|
| 1.1 | Airborne particles/dust | M | H | **M** | 1.32 | Software failure | M | VH | **H** |
| 1.2 | Air conditioning failure | M | VH | **H** | 1.33 | Staff shortage | M | H | **M** |
| 1.3 | Bomb Attack | L | VH | **M** | 1.34 | Theft | M | H | **M** |
| 1.4 | Communications infiltration | M | VH | **H** | 1.35 | Traffic overloading | M | H | **M** |
| 1.5 | Damage to communication lines/cables | L | H | **L** | 1.36 | Transmission errors | M | M | **L** |
| 1.6 | Deterioration of storage media | L | VH | **M** | 1.37 | Unauthorised use of software | M | H | **M** |
| 1.7 | Earthquake | L | H | **L** | 1.38 | Unauthorised use of storage media | M | M | **L** |
| 1.8 | Eavesdropping | M | H | **M** | 1.39 | Use of network facilities in an unauthorised way | M | H | **M** |
| 1.9 | Environmental contamination (and other forms of natural or man-made disasters) | L | H | **L** | 1.40 | Use of software by unauthorised users | M | H | **M** |
| 1.10 | Extremes of temperature and humidity | M | M | **L** | 1.41 | Use of software in an unauthorised way | M | H | **M** |
| 1.11 | Failure of communications services | M | H | **M** | 1.42 | User error | M | M | **L** |
| 1.12 | Failure of network components | M | H | **M** | 1.43 | Willful damage | M | H | **M** |
| 1.13 | Failure of power supply | L | VH | **M** | | | | | |
| 1.14 | Failure of water supply | L | M | **VL** | | | | | |
| 1.15 | Fire | M | VH | **H** | | | | | |
| 1.16 | Flooding | L | H | **L** | | | | | |
| 1.17 | Hardware failure | M | H | **M** | | | | | |
| 1.18 | Hurricane | L | H | **L** | | | | | |
| 1.19 | Illegal import/export of software | H | H | **H** | | | | | |
| 1.20 | Illegal use of software | H | H | **H** | | | | | |
| 1.21 | Industrial action | M | H | **M** | | | | | |
| 1.22 | Lightning | M | H | **M** | | | | | |
| 1.23 | Maintenance error | M | H | **M** | | | | | |
| 1.24 | Malicious software (eg. Viruses, worms, Trojan horses) | H | H | **H** | | | | | |
| 1.25 | Masquerading of user identity | M | H | **M** | | | | | |
| 1.26 | Misrouting or rerouting of messages | M | H | **M** | | | | | |
| 1.27 | Misuse of resources | M | VH | **H** | | | | | |
| 1.28 | Network access by unauthorised persons | M | VH | **H** | | | | | |
| 1.29 | Operational support staff error | M | H | **M** | | | | | |
| 1.30 | Power fluctuation | M | H | **M** | | | | | |
| 1.31 | Repudiation (eg. Of services, transactions, sending/receiving messages) | M | H | **M** | | | | | |

# 10. Catalogue of Vulnerabilities

| Ref | Vulnerability | Ease of Exploitation | Ref | Vulnerability | Ease of Exploitation |
|---|---|---|---|---|---|
| 2.1 | Absence of personnel | M | 2.30 | Complicated user interface | L |
| 2.2 | Unsupervised work by outside or cleaning staff | M | 2.31 | Disposal or reuse of storage media without proper erasure | M |
| 2.3 | Insufficient security training | L | 2.32 | Lack of audit trail | H |
| 2.4 | Lack of security awareness | L | 2.33 | Lack of documentation | M |
| 2.5 | Poorly documented software | M | 2.34 | Lack of effective change control | H |
| 2.6 | Lack of monitoring mechanisms | H | 2.35 | Lack of identification and authentication mechanisms | H |
| 2.7 | Lack of policies for the correct use of telecommunications media and messaging | H | 2.36 | No 'logout' when leaving the work station | H |
| 2.8 | Inadequate recruitment procedures | M | 2.37 | No or insufficient software testing | M |
| 2.9 | Inadequate or careless use of physical access control to buildings, rooms and offices | M | 2.38 | Poor password management (easily guessable passwords, storing of passwords, insufficient frequency of change) | H |
| 2.10 | Lack of physical protection for the building, doors and windows | M | 2.39 | Unclear or incomplete specification for developers | M |
| 2.11 | Location in an area susceptible to flood | H | 2.40 | Uncontrolled downloading and using software | VH |
| 2.12 | Unprotected storage | M | 2.41 | Unprotected password tables | M |
| 2.13 | Insufficient maintenance/faulty installation of storage media | M | 2.42 | Well known flaws in the software | L |
| 2.14 | Lack of periodic equipment replacement schemes | M | 2.43 | Wrong allocation of access rights | H |
| 2.15 | Susceptibility of equipment to humidity, dust, soiling | L | 2.44 | Insufficient or irregular water supply | M |
| 2.16 | Susceptibility of equipment to temperature variations | M | | | |
| 2.17 | Susceptibility of equipment to voltage variations | L | | | |
| 2.18 | Unstable power grid | M | | | |
| 2.19 | Unprotected communication lines | M | | | |
| 2.20 | Poor joint cabling | L | | | |
| 2.21 | Lack of identification and authentication mechanisms | H | | | |
| 2.22 | Lack of proof of sending or receiving messages | M | | | |
| 2.23 | Dial up lines | H | | | |
| 2.24 | Unprotected sensitive traffic | M | | | |
| 2.25 | Single point of failure | M | | | |
| 2.26 | Inadequate network management | H | | | |
| 2.27 | Lack of care at disposal | M | | | |
| 2.28 | Uncontrolled copying | M | | | |
| 2.29 | Unprotected public network connections | H | | | |

# 11. Ranking of Threat by Measure of Risk

To assist in the overall risk analysis process, the following procedure/table permits different threats with differing impacts and likelihoods of occurrence (taking account of vulnerability aspects) to be compared and ranked in order of priority. It should be noted that the Likelihood of Threat Occurrence may differ from site to site and over time – these will be re-assessed on a regular basis.

| Threat Ref. | Threat Descriptor | Impact (Asset) Value | Likelihood of Threat Occurrence | Measure of Risk | Threat Ranking |
|---|---|---|---|---|---|
| 1.19 | Illegal import/export of software | 5 | 4 | 20 | 1 |
| 1.20 | Illegal use of software | 5 | 4 | 20 | 1 |
| 1.24 | Malicious software (eg. Viruses, worms, Trojan horses) | 4 | 4 | 16 | 2 |
| 1.1 | Airborne particles/dust | 5 | 3 | 15 | 3 |
| 1.2 | Air conditioning failure | 5 | 3 | 15 | 3 |
| 1.4 | Communications infiltration | 5 | 3 | 15 | 3 |
| 1.8 | Eavesdropping | 5 | 3 | 15 | 3 |
| 1.11 | Failure of communications services | 5 | 3 | 15 | 3 |
| 1.12 | Failure of network components | 5 | 3 | 15 | 3 |
| 1.17 | Hardware failure | 5 | 3 | 15 | 3 |
| 1.25 | Masquerading of user identity | 5 | 3 | 15 | 3 |
| 1.28 | Network access by unauthorised persons | 5 | 3 | 15 | 3 |
| 1.30 | Power fluctuation | 5 | 3 | 15 | 3 |
| 1.36 | Transmission errors | 5 | 3 | 15 | 3 |
| 1.40 | Use of software by unauthorised users | 5 | 3 | 15 | 3 |
| 1.41 | Use of software in an unauthorised way | 5 | 3 | 15 | 3 |
| 1.43 | Willful damage | 5 | 3 | 15 | 3 |
| 1.10 | Extremes of temperature and humidity | 4 | 3 | 12 | 4 |
| 1.15 | Fire | 4 | 3 | 12 | 4 |
| 1.21 | Industrial action | 4 | 3 | 12 | 4 |
| 1.22 | Lightning | 4 | 3 | 12 | 4 |
| 1.23 | Maintenance error | 4 | 3 | 12 | 4 |
| 1.26 | Misrouting or rerouting of messages | 4 | 3 | 12 | 4 |
| 1.27 | Misuse of resources | 4 | 3 | 12 | 4 |
| 1.31 | Repudiation (eg. Of services, transactions, sending/receiving messages) | 4 | 3 | 12 | 4 |
| 1.32 | Software failure | 4 | 3 | 12 | 4 |

| Threat Ref. | Threat Descriptor | Impact (Asset) Value | Likelihood of Threat Occurrence | Measure of Risk | Threat Ranking |
|---|---|---|---|---|---|
| 1.34 | Theft | 4 | 3 | 12 | 4 |
| 1.37 | Unauthorised use of software | 4 | 3 | 12 | 4 |
| 1.13 | Failure of power supply | 5 | 2 | 10 | 5 |
| 1.29 | Operational support staff error | 3 | 3 | 9 | 6 |
| 1.33 | Staff shortage | 3 | 3 | 9 | 6 |
| 1.35 | Traffic overloading | 3 | 3 | 9 | 6 |
| 1.38 | Unauthorised use of storage media | 3 | 3 | 9 | 6 |
| 1.39 | Use of network facilities in an unauthorised way | 3 | 3 | 9 | 6 |
| 1.42 | User error | 3 | 3 | 9 | 6 |
| 1.5 | Damage to communication lines/cables | 4 | 2 | 8 | 7 |
| 1.6 | Deterioration of storage media | 4 | 2 | 8 | 7 |
| 1.9 | Environmental contamination (and other forms of natural or man-made disasters) | 4 | 2 | 8 | 7 |
| 1.16 | Flooding | 5 | 2 | 10 | 7 |
| 1.3 | Bomb Attack | 3 | 2 | 6 | 8 |
| 1.7 | Earthquake | 3 | 2 | 6 | 8 |
| 1.14 | Failure of water supply | 3 | 2 | 6 | 8 |
| 1.18 | Hurricane | 5 | 0 | 0 | 9 |

# 12. Reducing the Risks

The following table indicates the ways in which the controls selected by the Trust (ref. NHS TRUST Statement of Applicability Version 1.4) reduce the risks.

Controls can reduce the assessed risks in one of the following ways:

- Avoid the risk **(A)**
- Transfer the risk **(T)**
- Reduce the threats **(R)**
- Reduce the vulnerabilities **(V)**
- Reduce the possible impacts **(I)**
- Detect unwanted events, react and recover from them **(D)**

| BS7799-2:1999 Clause | BS7799-2:1999 Control Subject | Selected | Risk Reduction |
|---|---|---|---|
| BS7799-2 §4.1.1.1 | Information Security Policy Document | **Y** | **R,V** |
| BS7799-2 §4.1.1.2 | Review and Evaluation | **Y** | **R,V** |
| BS7799-2 §4.2.1.1 | Management Information Security Forum | **Y** | **R,V** |
| BS7799-2 §4.2.1.2 | Information Security Co-ordination | **Y** | **R,V** |
| BS7799-2 §4.2.1.3 | Allocation of Information Security responsibilities | **Y** | **R,V** |
| BS7799-2 §4.2.1.4 | Authorisation Process for Information Processing Facilities | **Y** | **R,V** |
| BS7799-2 §4.2.1.5 | Specialist Information Security Advice | **Y** | **R,V** |
| BS7799-2 §4.2.1.6 | Co-operation Between Organisations | **Y** | **R,V** |
| BS7799-2 §4.2.1.7 | Independent review of IS Security | **Y** | **R,V** |
| BS7799-2 §4.2.2.1 | Identification of Risks from Third Party Access | **Y** | **A,R,V** |
| BS7799-2 §4.2.2.2 | Security Requirements in Third Party Contracts | **Y** | **A,R,V** |
| BS7799-2 §4.2.3.1 | Security Requirements in Outsourcing Contracts | **N** | **N/a** |
| BS7799-2 §4.3.1.1 | Inventory of Assets | **Y** | **A,R,V** |
| BS7799-2 §4.3.2.1 | Classification Guidelines | **Y** | **R,V** |

| BS7799-2:1999 Clause | BS7799-2:1999 Control Subject | Selected | Risk Reduction |
|---|---|---|---|
| BS7799-2 §4.3.2.2 | Information Labelling and Handling | **Y** | **R,V** |
| BS7799-2 §4.4.1.1 | Including Security in Job Responsibilities | **Y** | **R,V** |
| BS7799-2 §4.4.1.2 | Personnel Screening and Policy | **Y** | **R,V** |
| BS7799-2 §4.4.1.3 | Confidentiality Agreements | **Y** | **R,V** |
| BS7799-2 §4.4.1.4 | Terms and Conditions of Employment | **Y** | **R,V** |
| BS7799-2 §4.4.2.1 | Information Security Education and Training | **Y** | **R,V** |
| BS7799-2 §4.4.3.1 | Reporting Security Incidents | **Y** | **R,V,D** |
| BS7799-2 §4.4.3.2 | Reporting Security Weaknesses | **Y** | **R,V,D** |
| BS7799-2 §4.4.3.3 | Reporting Software Malfunctions | **Y** | **R,V,D** |
| BS7799-2 §4.4.3.4 | Learning from Incidents | **Y** | **R,V,D** |
| BS7799-2 §4.4.3.5 | Disciplinary Process | **Y** | **R,V,D** |
| BS7799-2 §4.5.1.1 | Physical Security Perimeter | **Y** | **A,R,V** |
| BS7799-2 §4.5.1.2 | Physical Entry Controls | **Y** | **A,R,V** |
| BS7799-2 §4.5.1.3 | Securing Offices, Rooms and Facilities | **Y** | **A,R,V** |
| BS7799-2 §4.5.1.4 | Working in Secure Areas | **Y** | **A,R,V** |
| BS7799-2 §4.5.1.5 | Isolated Loading and Delivery Areas | **N** | **N/a** |
| BS7799-2 §4.5.2.1 | Equipment Siting and protection | **Y** | **A,R,V** |
| BS7799-2 §4.5.2.2 | Power Supplies | **Y** | **A,R,V** |
| BS7799-2 §4.5.2.3 | Cabling Security | **Y** | **A,R,V** |
| BS7799-2 §4.5.2.4 | Equipment Maintenance | **Y** | **A,R,V** |
| BS7799-2 §4.5.2.5 | Security of Equipment Off-premises | **Y** | **A,R,V** |
| BS7799-2 §4.5.2.6 | Secure Disposal or Re-use of Equipment | **Y** | **A,R,V** |
| BS7799-2 §4.5.3.1 | Clear Desk and Clear Screen Policy | **Y** | **R,V** |
| BS7799-2 §4.5.3.2 | Removal of Property | **Y** | **R,V** |
| BS7799-2 §4.6.1.1 | Documented Operating Procedures | **Y** | **R,V** |
| BS7799-2 §4.6.1.2 | Operational Change Control | **Y** | **R,V** |
| BS7799-2 §4.6.1.3 | Incident Management Procedures | **Y** | **R,V** |
| BS7799-2 §4.6.1.4 | Segregation of Duties | **Y** | **R,V** |
| BS7799-2 §4.6.1.5 | Separation of Development and Operational Facilities | **Y** | **R,V** |
| BS7799-2 §4.6.1.6 | External Facilities Management | **N** | **N/a** |
| BS7799-2 §4.6.2.1 | Capacity Planning | **Y** | **A,R,V** |
| BS7799-2 §4.6.2.2 | System Acceptance | **Y** | **A,R,V** |

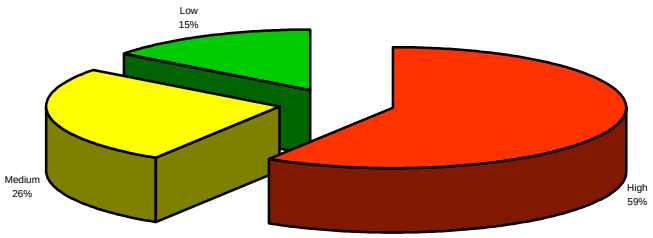
| BS7799-2:1999 Clause | BS7799-2:1999 Control Subject | Selected | Risk Reduction |
|---|---|---|---|
| BS7799-2 §4.6.3.1 | Controls Against Malicious Software | **Y** | **R,V,D** |
| BS7799-2 §4.6.4.1 | Information Backup | **Y** | **R,V** |
| BS7799-2 §4.6.4.2 | Operator Logs | **Y** | **R,V** |
| BS7799-2 §4.6.4.3 | Fault Logging | **Y** | **R,V,D** |
| BS7799-2 §4.6.5.1 | Network Controls | **Y** | **R,V** |
| BS7799-2 §4.6.6.1 | Management of Removable Computer Media | **Y** | **R,V** |
| BS7799-2 §4.6.6.2 | Disposal of Media | **Y** | **R,V** |
| BS7799-2 §4.6.6.3 | Information Handling procedures | **Y** | **R,V** |
| BS7799-2 §4.6.6.4 | Security of System Documentation | **Y** | **R,V** |
| BS7799-2 §4.6.7.1 | Information and Software Exchange Agreements | **Y** | **R,V** |
| BS7799-2 §4.6.7.2 | Security of Media in Transit | **Y** | **R,V** |
| BS7799-2 §4.6.7.3 | Electronic Commerce Security | **N** | **N/a** |
| BS7799-2 §4.6.7.4 | Security of Electronic Mail | **Y** | **A,R,V,D** |
| BS7799-2 §4.6.7.5 | Security of Electronic Office Systems | **Y** | **A,R,V,D** |
| BS7799-2 §4.6.7.6 | Publicly Available Systems | **Y** | **R,V,D** |
| BS7799-2 §4.6.7.7 | Other Forms of Information Exchange (voice, fax & video comms) | **Y** | **R,V,D** |
| BS7799-2 §4.7.1.1 | Access Control Policy | **Y** | **R,V,D** |
| BS7799-2 §4.7.2.1 | User Registration | **Y** | **R,V** |
| BS7799-2 §4.7.2.2 | Privilege Management | **Y** | **R,V,D** |
| BS7799-2 §4.7.2.3 | User Password Management | **Y** | **R,V,D** |
| BS7799-2 §4.7.2.4 | Review of User Access Rights | **Y** | **R,V** |
| BS7799-2 §4.7.3.1 | Password Use | **Y** | **R,V** |
| BS7799-2 §4.7.3.2 | Unattended User Equipment | **Y** | **R,V** |
| BS7799-2 §4.7.4.1 | Policy on Use of Network Services | **Y** | **R,V** |
| BS7799-2 §4.7.4.2 | Enforced Path | **Y** | **R,V** |
| BS7799-2 §4.7.4.3 | User Authentication for External Connections | **Y** | **R,V** |
| BS7799-2 §4.7.4.4 | Node Authentication | **N** | **N/a** |
| BS7799-2 §4.7.4.5 | Remote Diagnostic Port Protection | **Y** | **R,V** |
| BS7799-2 §4.7.4.6 | Segregation in Networks | **Y** | **R,V** |
| BS7799-2 §4.7.4.7 | Network Connection Control | **Y** | **R,V** |
| BS7799-2 §4.7.4.8 | Network Routing Control | **Y** | **R,V** |

| BS7799-2:1999 Clause | BS7799-2:1999 Control Subject | Selected | Risk Reduction |
|---|---|---|---|
| | | | |
| BS7799-2 §4.7.4.9 | Security of Network Services | **Y** | **R,V** |
| BS7799-2 §4.7.5.1 | Automatic Terminal Identification | **N** | **N/a** |
| BS7799-2 §4.7.5.2 | Terminal Log-on Procedures | **Y** | **R,V** |
| BS7799-2 §4.7.5.3 | User Identification and Authentication | **Y** | **R,V** |
| BS7799-2 §4.7.5.4 | Password Management System | **Y** | **R,V** |
| BS7799-2 §4.7.5.5 | Use of System Utilities | **Y** | **R,V** |
| BS7799-2 §4.7.5.6 | Duress Alarm to Safeguard Users | **N** | **N/a** |
| BS7799-2 §4.7.5.7 | Terminal Time-Out | **Y** | **R,V** |
| BS7799-2 §4.7.5.8 | Limitation of Connection Time | **Y** | **R,V** |
| BS7799-2 §4.7.6.1 | Information Access Restriction | **Y** | **R,V** |
| BS7799-2 §4.7.6.2 | Sensitive System Isolation | **N** | **N/a** |
| BS7799-2 §4.7.7.1 | Event Logging | **Y** | **R,V,D** |
| BS7799-2 §4.7.7.2 | Monitoring System Use | **Y** | **R,V,D** |
| BS7799-2 §4.7.7.3 | Clock Synchronisation | **Y** | **R,V** |
| BS7799-2 §4.7.8.1 | Mobile Computing | **Y** | **R,V** |
| BS7799-2 §4.7.8.2 | Teleworking | **N** | **N/a** |
| BS7799-2 §4.8.1.1 | Security Requirements Analysis and Specification | **N** | **N/a** |
| BS7799-2 §4.8.2.1 | Input Data Validation | **N** | **N/a** |
| BS7799-2 §4.8.2.2 | Control of Internal Processing | **N** | **N/a** |
| BS7799-2 §4.8.2.3 | Message Authentication | **N** | **N/a** |
| BS7799-2 §4.8.2.4 | Output Data Validation | **N** | **N/a** |
| BS7799-2 §4.8.3.1 | Policy on the Use of Cryptographic Controls | **N** | **N/a** |
| BS7799-2 §4.8.3.2 | Encryption | **N** | **N/a** |
| BS7799-2 §4.8.3.3 | Digital Signatures | **N** | **N/a** |
| BS7799-2 §4.8.3.4 | Non-Repudiation Services | **N** | **N/a** |
| BS7799-2 §4.8.3.5 | Key Management | **N** | **N/a** |
| BS7799-2 §4.8.4.1 | Control of Operational Software | **Y** | **R,V,D** |
| BS7799-2 §4.8.4.2 | Protection of System Test Data | **N** | **N/a** |
| BS7799-2 §4.8.4.3 | Access Control to Program Source Library | **Y** | **R,V,D** |
| BS7799-2 §4.8.5.1 | Change Control Procedures | **Y** | **R,V,D** |

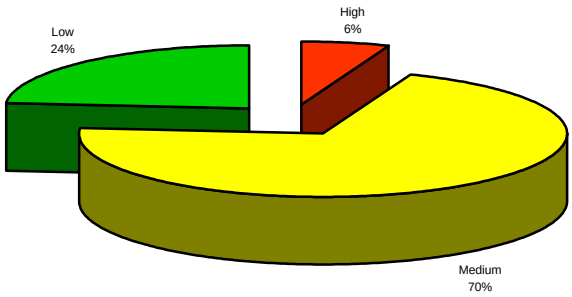
| BS7799-2:1999 Clause | BS7799-2:1999 Control Subject | Selected | Risk Reduction |
|---|---|---|---|
| BS7799-2 §4.8.5.2 | Technical Review of Operating Systems Changes | **Y** | **R,V,D** |
| BS7799-2 §4.8.5.3 | Restrictions to Changes to Software Packages | **N** | **N/a** |
| BS7799-2 §4.8.5.4 | Covert Channels and Trojan Code | **Y** | **R,V,D** |
| BS7799-2 §4.8.5.5 | Outsourced Software Development | **N** | **N/a** |
| BS7799-2 §4.9.1.1 | Business Continuity Management process | **Y** | **A,T,R,V,D** |
| BS7799-2 §4.9.1.2 | Business Continuity and Impact Analysis | **Y** | **A,T,R,V,D** |
| BS7799-2 §4.9.1.3 | Writing and Implementing Continuity Plans | **Y** | **A,T,R,V,D** |
| BS7799-2 §4.9.1.4 | Business Continuity Planning Framework | **Y** | **A,T,R,V,D** |
| BS7799-2 §4.9.1.5 | Testing, Maintaining and Re-Assessing Business Continuity Plans | **Y** | **A,T,R,V,D** |
| BS7799-2 §4.10.1.1 | Identification of Applicable Legislation | **Y** | **A,R,V,D** |
| BS7799-2 §4.10.1.2 | Intellectual Property Rights<br>a) Copyright<br>b) Software Copyright | **Y** | **A,R,V,D** |
| BS7799-2 §4.10.1.3 | Safeguarding of Organisational Records | **Y** | **A,R,V,D** |
| BS7799-2 §4.10.1.4 | Data Protection and Privacy of Personal Information | **Y** | **A,R,V,D** |
| BS7799-2 §4.10.1.5 | Prevention of Misuse of Information Processing Facilities | **Y** | **A,R,V,D** |
| BS7799-2 §4.10.1.6 | Regulation of Cryptographic Controls | **N** | **N/A** |
| BS7799-2 §4.10.1.7 | Collection of Evidence<br>a) Rules for Evidence<br>b) Admissibility of Evidence<br>c) Quality & Completeness of Evidence | **N** | **N/a** |
| BS7799-2 §4.10.2.1 | Compliance With Security Policy | **Y** | **A,R,V** |
| BS7799-2 §4.10.2.2 | Technical Compliance Checking | **Y** | **A,R,V** |
| BS7799-2 §4.10.3.1 | System Audit Controls | **Y** | **A,R,V** |
| BS7799-2 §4.10.3.2 | Protection of System Audit Tools | **N** | **N/a** |

# 13.Risk Assessment Review

## 14.1 Pre Implementation of Controls




## 14.2 Post Implementation of Controls




After implementation of the controls described more fully in the NHS TRUST Statement of Applicability Version x.x, there remains 6% of the total number of risks that are classified as Medium Likelihood/High Impact. There also remain 9% of the total number of risks that are classified as Medium Likelihood/Medium Impact and 62% of the total number of risks that are considered Low Likelihood/High Impact.

The Trust has determined that all residual risks classified as Low Likelihood/High Impact be determined as acceptable risks for the business to bear.

The Medium Likelihood/High Impact and Medium Likelihood/Medium Impact residual risks are considered more fully in the following section (section 14).

# 14. Unacceptable Residual Risks

| Residual Risks | Likelihood | Impact | Further Controls |
|---|---|---|---|
| Connections from external networks, undetected intrusions, fraud, industrial espionage, reputation and public confidence | Medium | High | Introduce regular reviews and attempted, unauthorised access trials. |
| Assets that are not classified correctly will receive an incorrect level of protection | Medium | Medium | Ensure continued adherence to the NHS classification guidelines |
| Security incidents and malfunctions are not responded to correctly, they are not reported and hence no corrective action can be taken resulting in potential disruption to business. | Medium | High | Strengthen the employee/ contractor induction team briefing processes |
| Lack of adequate awareness of responsibilities and the value of information assets can lead to security breaches due to carelessness or lack of knowledge. | Medium | Medium | Strengthen the employee/ contractor induction team briefing processes |
| Unauthorised access will go undetected, capacity inappropriate to use, performance degradation | Medium | Medium | Monitor system performance on a regular basis and report to the Director of Finance and IT |
| Unauthorised access to information assets (this includes mobile/homeworkers even though their access controls include Secure ID, pin number and password processes). | Medium | High | Express reminders to everyone during Information Security induction and refresher training and specific monitoring of mobile/homeworker access. |

The above residual risks are reviewed on a monthly basis to ensure the additional controls are having an effect on the Likelihood rating (Impact is deemed not to change). Any improvement to Likelihood (ie. medium to low) will result in the residual risk becoming an acceptable residual risk.

# 15. Summary – Impact/Likelihood Analysis

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| **The Trust does not have a Security policy or that it is poorly written.** | **High** | **Medium** | The policy is approved, published and communicated to all employees and is contained within the NHS TRUST Information Security – A Guide for Staff | ***Security Policy*** | *To demonstrate management's commitment and set out the organisation's approach to managing information security, distributed to every employee.* | **Low** |
| **The Trust do not have an Information Security Infrastructure or that it does not work satisfactorily.** | **High** | **Medium** | The management framework is established to initiate and control the implementation and ongoing effectiveness of Information Security. | ***Information Security Infrastructure*** | *To manage information security within the Trust.* | **Low** |
| **Connections from external networks, undetected intrusions, fraud, industrial espionage, reputation and public confidence** | **High** | **High** | Controls for the Security of Third Party Access are developed. | ***Security of Third Party Access*** | *To maintain the security of organisational information processing facilities and information assets accessed by third parties.* | **Medium** |
| **Loss and theft of computer hardware and unlawful copying of software** | **Low** | **Medium** | All major information assets are accounted for and have a nominated owner. | ***Accountability for Assets*** | *To maintain appropriate protection of organisational assets.* | **Low** |
| **Assets that are not classified correctly will** | **Medium** | **Medium** | Information is classified to indicate the need, priorities and degree of | ***Information Classification*** | *To ensure that information assets receive an* | **Medium** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| **receive an incorrect level of protection.** | | | Information Classification required | | *appropriate level of protection* | |
| **Accountability not understood by employee/contractors.** | **Medium** | **Low** | This is clearly defined and responsibilities are addressed at the recruitment stage, are included in contracts and are monitored during an individual's employment. | ***Security in Job Definition and Resourcing*** | *To reduce the risks of human error, theft, fraud or misuse of facilities* | **Low** |
| **Users do not understand information security threats and concerns and are not able to support the security policy giving rise to breaches of security.** | **Medium** | **Medium** | Users are trained in security procedures and the correct use of information processing facilities to minimise possible security risks. | ***User Training*** | *To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.* | **Low** |
| **Security incidents and malfunctions are not responded to correctly, they are not reported and hence no corrective action can be taken resulting in potential disruption to business.** | **High** | **Medium** | Incidents affecting security are reported through appropriate channels as quickly as possible. | ***Responding to Security Incidents And Malfunctions*** | *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* | **Medium** |
| **Unauthorised access providing the opportunity to cause major damage** | **High** | **Low** | Critical or sensitive business Information processing facilities are housed in Secure Areas, protected by defined Security perimeter with | ***Secure Areas*** | *To prevent unauthorised access, damage and interference to business premises and information.* | **Low** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| **and to become aware of confidential information.** | | | appropriate security barriers and entry controls. They are physically protected from unauthorised access, damage and interference. | | | |
| **Assets are lost, damaged or compromised thus causing interruption to the business.** | **Medium** | **Low** | Equipment is physically protected from security threats and environmental hazards by the use of secured rooms/offices, locked cabinets and authorised access control. Policies exist for portable equipment. | ***Equipment Security*** | *To prevent loss, damage or compromise of assets and interruption to business activities* | **Low** |
| **Disclosure to, modification of or theft, by unauthorised persons could cause loss or damage to information processing facilities.** | **Medium** | **Medium** | Information and information processing facilities are protected from disclosure to, modification of or theft by, unauthorised person, and controls are in place to minimise loss or damage. | ***General Controls*** | *To prevent compromise or theft of information and information processing facilities.* | **Low** |
| **Incorrect operation of information processing facilities thus causing potential for business disruption.** | **High** | **Low** | Responsibilities and procedures for the management and operation of all information processing facilities are established. They include the development of appropriate operating instructions and incident response procedures. Segregation of duties are implemented where appropriate. | ***Operational Procedures and Responsibilities*** | *To ensure the correct and secure operation of information processing facilities.* | **Low** |
| **Lack of planning will lead to systems failures.** | **High** | **Medium** | Advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity are made, to reduce the risk of system | ***System Planning and Acceptance*** | *To minimise the risk of systems failures.* | **Low** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| | | | overload. | | | |
| **Desktop and central systems become inoperable.** | **High** | **High** | Software and information processing facilities are vulnerable to the introduction of malicious software such as viruses, network worms, Trojan horses and logic bombs. There are formal precautions in place to provide the required level of protection. | ***Protection Against Malicious Software***. | *To protect the integrity of software and information.* | **Low** |
| **Information and communication services become unavailable and/or data integrity is compromised.** | **High** | **Medium** | Routine procedures are established for carrying out the agreed backup strategy, taking backup copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment. | ***Housekeeping*** | *To maintain the integrity and availability of information processing and communication services.* | **Low** |
| **Unauthorised access to information and/or malicious damage to the network infrastructure.** | **High** | **Medium** | A range of controls are in place to achieve and maintain security in computer networks which span organisational boundaries. | ***Network Management*** | *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.* | **Low** |
| **Assets are damaged and/or information is compromised or unavailable** | **Medium** | **Low** | Media is controlled and physically protected. | ***Media Handling and Security*** | *To prevent damage to assets and interruptions to business activities.* | **Low** |
| **Information is accessed by unauthorised personnel thus exposing the organisation to harm.** | **High** | **Medium** | Access to information, and business Processes is controlled on the basis of Business and security requirements. This takes into account policies for information dissemination and authorisation. | ***Business Requirement for Access Control*** | *To control access to information.* | **Low** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| | | | | | | |
| **Information is accessed by unauthorised personnel thus exposing the organisation to harm.** | **High** | **Medium** | Formal procedures are in place to control the allocation of access rights to information systems and services. | ***User Access Management*** | *To prevent unauthorised access to information systems.* | **Low** |
| **Lack of adequate awareness of responsibilities and the value of information assets can lead to security breaches due to carelessness or lack of knowledge.** | **Medium** | **Medium** | The co-operation of authorised users is essential for effective security. Users are made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. | ***User Responsibilities*** | *To prevent unauthorised user access.* | **Medium** |
| **Unauthorised access to networks and hence information.** | **High** | **Medium** | Access to both internal and external networked services is controlled. | ***Network Access Control*** | *To provide protection of networked services.* | **Low** |
| **Unauthorised access to computer resources and hence information.** | **High** | **Medium** | Security facilities at the operating system level are used to restrict access to computer resources. | ***Operating System Access Control*** | *To prevent unauthorised computer access.* | **Low** |
| **Unauthorised access to application systems and hence information.** | **High** | **Medium** | Security facilities are used to restrict Access within application systems. Logical access to software and Information is restricted to authorised users. | ***Application Access Control*** | *To prevent unauthorised access to information held in information systems.* | **Low** |
| **Unauthorised access will** | **Medium** | **Medium** | Systems are monitored to detect Deviation from access control policy | ***Monitoring*** | *To detect unauthorised activities, to enable capacity* | **Medium** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| **go undetected, capacity inappropriate to use, performance degradation** | | | and record monitorable events to provide evidence in case of security incidents. | ***System Access and Use*** | *planning and to monitor performance* | |
| **Unauthorised access to information assets.** | **High** | **High** | When using mobile computing the risks of working in an unprotected environment are greater therefore appropriate additional protection is applied. | ***Mobile Computing and Teleworking*** | *To ensure information security when using mobile computing and teleworking facilities.* | **Medium** |
| **User data is lost, modified without authorisation or misused.** | **Medium** | **Low** | Appropriate controls and audit trails or Activity logs are built into application systems, including user written applications. These will include the validation of input data, internal processing and output data. | ***Security in Application Systems***. | *To prevent loss, modification or misuse of user data in application systems.* | **Low** |
| **Unauthorised access to systems and support activities.** | **High** | **Medium** | Access to system files is controlled. Maintaining system integrity is the responsibility of the user function or development group to whom the application system or software belongs. | ***Security of System Files*** | *To ensure IT projects and support activities are conducted in a secure manner.* | **Low** |
| **Disruption to the business.** | **High** | **Medium** | A business continuity management process is implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventative and recovery controls. | ***Aspects of Business Continuity Management***. | *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.* | **Low** |
| **Criminal and civil law, statutory, regularity or contractual obligations** | **High** | **Low** | The design, operation, use and management of information systems may be subject to statutory, regulatory | ***Compliance with Legal Requirements.*** | *To avoid breaches of any criminal and civil law, and statutory, regularity or* | **Low** |

| Risk | Impact | Pre-Strategy Likelihood | Strategy | Control | Objective | Post Strategy Likelihood |
|---|---|---|---|---|---|---|
| **and any security requirement are breached.** | | | and contractual security requirements. | | *contractual obligations, and any security requirements.* | |
| **Compliance is not maintained.** | **High** | **Medium** | The security of information systems will be regularly reviewed and records kept of all reviews. | ***Reviews of Security Policy and Technical Compliance.*** | *To ensure compliance of systems with organisational security policies and standards.* | **Low** |

# Appendix A – Threat, Vulnerability & Asset Value Matrix

## Measure of Risk

| | Levels of Threat | Very Low/Low | | | | Medium | | | | High | | | | Very High | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Levels of Vulnerability | L | M | H | VH | L | M | H | VH | L | M | H | VH | L | M | H | VH |
| Asset Value | VL/L | 0 | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 2 | 3 | 4 | 5 | 3 | 4 | 5 | 6 |
| | M | 1 | 2 | 3 | 4 | 2 | 3 | 4 | 5 | 3 | 4 | 5 | 6 | 4 | 5 | 6 | 7 |
| | H | 2 | 3 | 4 | 5 | 3 | 4 | 5 | 6 | 4 | 5 | 6 | 7 | 5 | 6 | 7 | 8 |
| | VH | 3 | 4 | 5 | 6 | 4 | 5 | 6 | 7 | 5 | 6 | 7 | 8 | 6 | 7 | 8 | 9 |

The matrix shown above has been used to determine the ‘Measure of Risk’ as detailed in section 8 of this manual (Inventory of Major Trust Information Assets). The matrix is 3 dimensional taking into account Threats, Vulnerabilities and Asset Value resulting in an overall ‘Measure of Risk’ in the range 0 (no risk) to 9 (very high risk).

# Appendix B – Inventory of Assets – Applications

| System Description | Value (VH/H/M/L) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# Appendix C – Inventory of Assets - Location/Server

| Location | Machine Name | Function | Domain | Server Type | Identifier | Value (VH/H/M/L) |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Appendix D – Inventory of Assets – Desktops/Laptops etc.

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Equipment | Make | Model | Serial Number | Users | Location | Asset Value |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Appendix E – WAN Schematic

# Appendix F – Wide Area Network Used by the NHS TRUST

## F1 Network Components

The WAN (Wide Area Network) as used by NHS is shown in Figure 1. It is made up of the following components:

1. Local users PC/Wyse Terminal
2. Network cabling
3. Network Hub/Switch
4. Local-site server
5. Cisco Router
6. NHSNet
7. Reading/Alfreton Cisco Router
8. BILLY Terminal Server
9. BILLY Data Server
10. BILLY PDC/BDC
11. BILLY Print Server
12. BILLY Mail Server
13. BILLY CD Tower

### Figure 1

# F2 – Connection Process

The connectivity process starts with the local user PC. This PC once switched on initializes its own Network connectivity software. This software allows it to talk to the LAN (Local Area Network), providing access to the Local-site server.

Once the pre-requisite conditions of connectivity have been met by the local site communication can take place. This means that IP communications packets can be routed out on to the WAN via the “BT managed” CISCO router.

Assuming that all goes well at the LAN end and the communications packets are being routed out onto the WAN, BT will route these packets to the appropriate destination either Alfreton or Reading. The communications packets will be routed in via the Alfreton/Reading site “BT managed” Cisco router and onto the LAN at that end. The communications packets will then be shared around the BILLY terminal servers, balancing the load as necessary.

# F3 - BILLY User Access

Physical connectivity to Billy is controlled by the Primary or Backup Domain Controllers. These ratify the username and passwords before allowing the user to logon at the terminal servers. The user logs on and connects to a Terminal Server where all his/her applications are setup for him/her to use. The Data resides on the data servers, mail resides on the mail server.

# F4 - Connectivity Issues and Pre-requisites

The communications path between PC and BILLY must include a connection to the local-site server, the site BT Managed Cisco router and consequently NHS Net. NhsNet must have connectivity to the distant BILLY Terminal Server farm via the end node BT managed Cisco Router.

The connectivity at the Local-site provided by the Server to the PC provides several services:

1. It supplies the PC/Wyse terminal its IP configuration details
2. It monitors the users BILLY configuration files and updates them as necessary
3. It provides C: drive anti-virus checking for Boot-sector viruses only.
4. It also provides backup connectivity software for RESUS in the event of BILLY failure.

# F5 - Connectivity Fault-finding Aids

A list of all sites and their IP addresses can be found on the technical web-site (see Figures 2 and 3). This is provided to you for fault diagnosis and reporting. If a report occurs of no connectivity for a site you must check this out immediately. Go to the technical web-site, get the IP address of the site and test the connectivity by pinging the site details found. If no response is found, you must book this to BT on xxxx xxxxxx, on reporting BT will only take notice if you supply the SIN details for the faulty site. Once reported successfully to BT they must repair the service within 4 hours or pay us money back.

## Figure 2

## Appendix F continued

# Figure 3

# Appendix G - Brief Description of the Trust's client/server approach

The approach is based upon Windows NT 4 Server Terminal Server Edition supported by xxxx Metaframe. These innovative products move a Windows NT Workstation environment from the desktop PC to a centralised collection of powerful servers.

The applications (for example Word) actually run on these centralised servers, which send only the screen update information back to the users desktop (client) machine. The result is a very low network communication requirement that functions well even over slow modems (the slowest tested so far is a 19.2k modem - far slower than most of those in used by most portable computers for dial in mail access). Even more impressive is the range of client systems that can connect to the centralised servers.

The system can be accessed from desktop or portable computer using Intel 80286 PC's upwards running DOS only, Windows 3.1, Windows 95/98, Windows NT Workstation, hand held "personal organisers" using Windows CE, many UNIX Workstations and dedicated "WinTerm" terminals. Each of these machines delivers full performance with complete Billy functionality.

Because the applications run on the centralised system, no network is involved when applications are loaded, resulting in a fast system response. The system implemented by NHS xxxxxxxx uses a number of Terminal Server machines based in two "server farms" located at separate sites.

These serve the whole of the country. Each of the Terminal Server machines contains two Intel Pentium III 450MHZ processors with 768MB of RAM. These are supplemented by highly resilient mail and data servers that provide a total of 200GB of data storage.

When a user connects to the Terminal Server "farm", they could connect to any one of a number of machines, perhaps a different one each session. Which machine they connect to is decided by load balancing software to ensure an even distribution of users and activity across the system. This independence provides a high degree of resilience. A failure in a terminal server machine will not significantly affect access to services or data.