

# Network Security Policy

**Version 4.0**

**March 2010**

<b>Category:</b>	Organisational Document
<b>Summary:</b>	The purpose of this Policy is to provide a clear security definition for the use of the Trust Network in a secure and professional manner.
<b>Equality and Impact Assessment undertaken:</b>	
<b>Date of Review:</b>	March 2011
<b>Approval Date/ Via:</b>	▪ March 2010 / Information Governance Group
<b>Distribution:</b>	Via Information Governance Manager to: <ul style="list-style-type: none"><li>▪ Divisional Directors and Directorate Managers</li><li>▪ Information Governance Intranet site</li></ul> Via PFI Client Contract Office to: <ul style="list-style-type: none"><li>▪ Carillion Health</li><li>▪ G4S</li></ul> Via Departmental Managers to: <ul style="list-style-type: none"><li>▪ Employees / 3<sup>rd</sup> party suppliers /support organisations</li></ul>
<b>Author(s):</b>	Information Protection Officer Information Security Manager
<b>Lead executive:</b>	Director of Planning and Information

### Introduction

This document defines the Network Security Policy for the Oxford Radcliffe Hospitals NHS Trust (the Trust). The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who use and/or support the network.. The Trust ICT Infrastructure is managed and supported by Oxfordshire Health Informatics Service (OHIS) however it is recognised that some ICT systems are managed by internal Trust departments. Where this is the case they must ensure compliance with this policy. OHIS provide connectivity and other ad-hoc IT support as defined within the OHIS Service Directory.

This document sets out the Trust's policy for the protection of the confidentiality, integrity and availability of the network. It establishes the responsibilities for network security and provides reference to documentation relevant to this policy.

### Aim

1. The aim of this policy is to ensure the security and continuous functioning of The Oxford Radcliffe Hospitals NHS Trust's ICT network managed by OHIS. To do this, OHIS will:
  - 1.1. Ensure availability of both infrastructure and connectivity.
  - 1.2. Ensure that the network is accessed only by authorised users.
  - 1.3. Preserve the Integrity of the network
  - 1.4. Protect the network from unauthorised access or modification.
  - 1.5. Ensure that the Preservation of Confidentiality is technically supported.
  - 1.6. Protect assets against unauthorised removal or disclosure.

### Network definition

2. The network is a collection of communication equipment such as servers, computers, printers, routers and switches, which has been connected together by cables or wireless. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment. It also enables centralised data backup, remote management of assets and automatic deployment of security tools e.g. anti-virus software.

### Scope of this Policy

3. This policy applies to all networks within the Trust used for:
  - 3.1. The storage, sharing and transmission of non-clinical data and images
  - 3.2. The storage, sharing and transmission of clinical data and images

- 3.3. Printing or scanning non-clinical or clinical data or images
- 3.4. The provision of NHS network or Internet systems for receiving, sending and storing non-clinical or clinical data or images
- 3.5. The provision of Remote access to internal systems via secure access such as N3 VPN.

### The Policy

4. The Trust ICT network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, the Trust will undertake to do the following.
  - 4.1. Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
  - 4.2. Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
  - 4.3. Implement the Network Security Policy in a consistent, timely and cost effective manner.
  - 4.4. Where relevant, the Trust will comply with:
    - 4.4.1. Copyright, Designs & Patents Act 1988
    - 4.4.2. Access to Health Records Act 1990
    - 4.4.3. Computer Misuse Act 1990
    - 4.4.4. The Data Protection Act 1998
    - 4.4.5. The Human Rights Act 1998
    - 4.4.6. Electronic Communications Act 2001
    - 4.4.7. Regulation of Investigatory Powers Act 2000
    - 4.4.8. Freedom of Information Act 2000
    - 4.4.9. Health & Social Care Act 2001
5. The Trust will comply with other laws, legislation and NHS policies and guidelines as appropriate.
6. The policy must be approved by the Information Security Manager (ISM).

### Risk Assessment

7. The Trust will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the

network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

8. Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the network.
9. Formal risk assessments will be conducted to ensure the network conforms to ISO27001 (ISO17799).

### **Physical & Environmental Security**

10. Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.
11. Responsibility should be recorded for ensuring that door lock codes are changed periodically, following a compromise of the code, or if the responsible person suspects the code has been compromised,
12. Critical or sensitive network equipment will be protected from power supply failures.
13. Critical or sensitive network equipment will be protected by intruder alarms and where possible fire suppression systems.
14. Smoking, eating and drinking is strictly controlled in areas housing critical or sensitive network equipment.
15. All visitors to secure network areas must be authorised by the OHIS Network Managers or the Head of IM&T Service Delivery.
16. All visitors to secure network areas must be made aware of network security requirements and evacuation procedures where fire suppression systems are in use.
17. All visitors to secure network areas must be logged in and out upon entering/leaving the building. The log will contain name, organisation, purpose of visit, date, and time in and out.
18. OHIS will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.
19. No person is to connect any device (PC, switch, hub, etc.) to the network without prior OHIS permission.

### **Access Control to Secure Network Areas**

20. Entry to secure areas housing critical or sensitive network equipment will be restricted to those who require access to carry out their jobs. Unsupervised access is

kept to a minimum and OHIS technical managers will maintain and periodically review a list of those with unsupervised access.

21. Under an agreement with OBMH, an allocation of equipment space has been provided in the OCDEM Data Centre for the sole use of OBMH. Designated OBMH IT staff have 24x7 access to this facility and have been provided with two security swipe cards to facilitate a secure and controlled access procedure. OBMH staff have been instructed in the procedure and in the necessary H&S and other procedures required to allow access to the Data Centre.

### **Access Control to the Network**

22. Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the Trust's Remote Access Policy.
23. User registration and de-registration procedure for access to the network is controlled directly by OHIS acting upon information provided by the Trust. This ensures only valid Trust employees and other authorised persons reside on the system. Ad-hoc accounts i.e. Contractors, are assigned an account end date when created.
24. Departmental line managers must approve user access for their staff.
25. Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
26. Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis, and at OHIS' discretion.
27. Access will not be granted until the HR system or an authorised administrator registers a user.
28. All users to the network will have their own individual user identification and password, except where the Trust has defined that generic usernames may be used.
29. Users are responsible for ensuring their password is kept secret (see User Responsibilities).
30. User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs.
31. Password changes will be forced on the user every 90 days with login denied after 3 attempts. This can be reset through the OHIS Service Desk or the automated Password Management tool.

### **Third Party Access Control to the Network**

32. Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.

33. All third party access to the network must be logged.

### **External Network Connections**

34. OHIS and the Trust will ensure that all connections to external networks and systems have documented and approved System Security Policies.
35. OHIS will ensure that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.
36. The Information Security Manager must approve all connections to external networks and systems before they commence operation.

### **Maintenance Contracts**

37. The Information Security Manager is responsible for ensuring that maintenance contracts are maintained and periodically reviewed for all network equipment.

### **Data and Software Exchange**

38. Formal agreements for the exchange of data and software between organisations must be established and approved by the Information Security Manager or relevant Directorate Manager.

### **Fault Logging**

39. The Information Security Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed. OHIS will operate ITIL-based Incident Management processes to record and track faults, and Problem and Change Management processes to review and implement countermeasures.

### **System Specific Policies**

40. OHIS and the Trust will introduce System Specific Policies and security contingency plans that reflect the Network Security Policy.
41. Changes to operating procedures must be authorised by the ISM or IAO for non-OHIS managed systems.

### **Network Operating Procedures**

42. Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation.
43. Changes to operating procedures must be authorised by the OHIS Head of IM&T Service Delivery.

### **Data Backup and Restoration**

44. The ISM is responsible for ensuring that backup copies of network configuration data are taken regularly.
45. Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant staff.
46. All backup tapes will be stored securely and where operationally possible a copy will be stored off-site.
47. Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
48. Users are responsible for ensuring that their own data is backed up by storing their data on the network server.
49. IAO are responsible for locally managed system backups.

### **User Responsibilities, Awareness & Training**

50. The Trust will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
51. All users of the network must be made aware of the contents and implications of the Network Security Policy and System Specific Policies.
52. Irresponsible or improper actions by users that compromise the confidentiality, availability and resilience of the network systems may result in disciplinary action(s).

### **Accreditation of Network Systems**

53. Ensure that the network is approved by the ISM before it commences operation. In this role the Network Managers will support the ISM. The Network Managers are responsible for ensuring that the network does not pose an unacceptable security risk to the organisation.

### **Security Audits**

54. The ISM and/or the Network Managers will require checks on, or an audit of, actual implementations based on approved security policies.

### **Malicious Software**

- 1.1. OHIS will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

### **Secure Disposal or Re-use of Equipment**

55. Where possible equipment will be reallocated if it is fit for purpose and supportable, otherwise OHIS will recommend that equipment reaching end-of-life will be replaced. Equipment replaced through OHIS will be securely disposed of and a certificate of destruction issued, to include data content. If a Trust department procures equipment independently (see section 7.10) that department will be responsible for the secure disposal of the replaced equipment, and a certificate of destruction must be obtained.

### **System Change Control**

56. The ISM may require checks on, or an assessment of the actual implementation based on the proposed changes.
57. The ISM is responsible for ensuring that selected hardware or software meets agreed security standards.
58. As part of acceptance testing of all new network systems, the Network Managers will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.
59. Testing facilities will where possible be used for all new network systems. Development and operational facilities will be separated where possible.

### **Security Monitoring**

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

### **Reporting Security Incidents & Weaknesses**

61. OHIS will record such incidents in the OHIS Call Management system (Helpmate) and all potential security breaches will be investigated and reported to non-clinical risk management. Security incidents and weaknesses must be reported in accordance with the requirements of The Trust's incident reporting procedure. Incidents involving non-OHIS-supported systems will be reported by the IAO.

### **System Configuration Management**

62. OHIS will ensure that there is an effective configuration management system for the network.

### **Business Continuity & Disaster Recovery Plans**

63. OHIS will ensure that business continuity plans and disaster recovery plans are produced for the network.
64. The plans must be reviewed by the ISM and tested on a regular basis.

### **Unattended Equipment and Clear Screen**

65. Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.
66. The Trust operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a password-protected screensaver activated if a workstation is left unattended for a short time.
67. Users failing to comply may be subject to disciplinary action.

### **Security Responsibilities**

68. The Chief Executive has delegated the overall security responsibility for security, policy and implementation to the ISM.
69. Responsibility for implementing this policy within the context of IT systems development and use in the organisation is delegated further to the OHIS Network Managers

### **Information Security Manager's Responsibilities**

70. Produce and implement effective security countermeasures.
71. Facilitate the production of all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Network Security Policy.
72. Act as a central point of contact on information security within the organisation, for both staff and external organisations.
73. Implement an effective framework for the management of security, i.e. implement an Information Security Management System supported by an Information Security Risk Treatment Plan
74. Assist in the formulation of Information Security Policy and related policies.
75. Advise on the content and implementation of the Information Security Programme.
76. Produce organisational standards, procedures and guidance on Information Security matters for approval by the Information Governance Steering Group.
77. Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
78. Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
79. These activities are carried out on behalf of and with Trust agreement.

### **Information Protection Officer's responsibilities**

---

80. Ensuring that appropriate Data Protection Act notifications are maintained for information stored on the network.
81. Dealing with enquires, from any source, in relation to the Data Protection Act and facilitating Subject Access Requests.
82. Advising users of information systems, applications and networks of their responsibilities under the Data Protection Act, including Subject Access.
83. Advising the Network Managers on breaches of the Act and recommended actions.
84. Encouraging, monitoring and checking compliance with the Data Protection Act.
85. Liaising with external organisations regarding Data Protection Act matters.
86. Promoting awareness and providing guidance and advice related to the Data Protection Act as it applies within the Trust.

### **Network Managers' Responsibilities**

87. Reporting to the Information Security Manager on matters relating to IT security.
88. Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
89. Representing the organisation on internal and external committees that relate to IT security.
90. Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
91. Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally by the Information Security Manager.
92. Ensuring that access to the organisation's network is limited to those who have the necessary authority and clearance.
93. Providing advice and guidance to development teams to ensure that the policy is complied with.
94. Approving system security policies for the infrastructure and common services.
95. Approving tested systems and agreeing rollout plans.
96. Advising the Information Security Manager on the accreditation of IT systems, applications and networks.
97. Providing a central point of contact on IT security issues.
98. Providing advice and guidance on:
  - 98.1. Policy Compliance
  - 98.2. Incident Investigation
  - 98.3. IT Security Awareness

- 98.4. IT Security Training
- 98.5. IT Systems Accreditation
- 98.6. Security of External Service Provision
- 98.7. Contingency Planning for IT systems
- 99. Contacting the Information Security Manager when:
  - 99.1. Incidents or alerts have been reported that may affect the organisation's systems, applications or networks.
  - 99.2. Proposals have been made to connect the organisation's systems, applications or networks to systems, applications or networks that are operated by external organisations.
  - 99.3. Passing on the advice of external sources/authorities on IT security matters.

### **Line Manager's Responsibilities**

- 100. Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- 101. Ensuring that their staff are made aware of their security responsibilities.
- 102. Ensuring that their staff have had suitable security training.
- 103. Ensuring that staff changes (starters and leavers) are notified to the appropriate systems managers so that access can be granted/removed.

### **General Responsibilities**

- 104. All personnel or agents acting for the organisation have a duty to:
- 105. Safeguard hardware, software and information in their care.
- 106. Prevent the introduction of malicious software on the organisation's IT systems.
- 107. Report on any suspected or actual breaches in security.

**Document History**

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Status</b>	<b>Comment</b>
3.0	February 2010	Robin Peach-Toon / Philip Pinney	Draft	Review and replacement of Version 2.0 Network Security Policy / Full rewrite of policy
	March 2010		Draft	Agreed by IGG subject to review by CEAC
	April 2010			Reviewed by Ian Thompson, CEAC auditor and forwarded to P Pinney
4.0	August 2010		Final	Received from P Pinney
4.0	August 2010		Final	Document re drafted into Trust format and placed on IGG intranet site 2/8/10 (KH)

**Next review: April 2011**