Warrington and Halton Hospitals NHS
NHS Foundation Trust

Third Party Relationships

Document History

Date	Version	Author	Changes
01/12/2009	1.0	Stephen Deacon	
04/03/2010	1.0		Document Approved: D Gallie
29/07/2010	2.0	Stephen Deacon	Adding additional IG requirements

Table of Contents

1. Introduction

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

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

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

This procedure outlines the way the Trust works with trusted third parties.

The following procedures are covered:

- Computer hardware and peripherals
- Software support
- Cleaning services

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Governance Team
Approval	Associate Director I.T.
Local adoption	Line Managers (in scope)
Compliance	All Staff and Contractors (in scope)
Monitoring	Information Governance Team

3. Computer Hardware and Peripherals

The Trust uses non-Trust support providers here to provide hardware and peripheral support; these are backed up by service level agreements. The services, reports and records provided by the third party are monitored and reviewed annually, unless the situation requires immediate attention. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed at each contract negations.

Hardware

Please see SS 03 Asset Management.doc for list of hardware support companies.

Detailed below are the terms and conditions the third parties must adhere to when gaining access to the Trust both electronically and physically.

3.1 Non-Disclosure Agreement

All third party business with the Trust shall be subject to the Terms of Offer, NHS Conditions of Contract. See Appendix A for section 35 of the NHS Conditions of Contract for the Supply of Services

3.2 Reporting of Information Security Events by Service Providers and Business Partner Organisations

Information security incidents should be reported to Warrington and Halton Hospitals NHS Foundation Trust and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur.

Definition of an Information Security Event
Incidents of theft, accidental loss or inappropriate disclosure of Warrington and Halton Hospitals Foundation Trust data should be reported to the relevant Information Asset Owner at the Trust. Procedural failure of equipment containing WHH data should also be reported to the Information Asset Owner responsible for the data.

How Information Security Events Need to Be Reported
In the first instance information security incidents should be reported to the Trust's IT Helpdesk 01925 662346. The incident will be dealt with in line with procedures contained within the Trust's Information Security Management System and it's Information Risk Policy.

3.3 Physical Access

IM&T Department:
The IM&T Department is a dedicated area only for IM&T staff. All non IM&T staff have to ring the bell/buzzer to gain access to the IM&T department. Non IM&T staff are not allowed into the department unsupervised. During Out-of-hours periods the main front door is locked.

3.4 Network Access

No third party contractor shall be given access to the Trust's network without the permission of any of the below senior IM&T Staff:

- Dave Gallie
- Steve Blake
- Phil Smith
- Joe Garnett
- Tracie Waterfield
- Brian Rigby
- Robbie Ryan
- Stephen Deacon
- Ivan Ostler

3.5 Hardware and Peripheral Removal

In the event that a piece of equipment needs to be taken off site for maintenance by a third party company all hard disks must be securely disposed of in accordance with the terms and conditions of their contract, and/or the NHS National Catalist framework. All confidential information is removed.

4. Software Support

To see who the Trust uses to provide software support, please view the ..\..\Applications_WHH Systems these are backed up by service level agreements.

Detailed below are the terms and conditions that third parties must adhere to when gaining access to the Trust both electronically and physically. The services, reports and records provided by the third party are monitored and reviewed annually, unless the situation requires immediate attention. Changes to the provision of services, including maintaining and

improving existing information security policies, procedures and controls, are managed at each contract negations.

4.1 Non-Disclosure Agreement

All third party business with the Trust sign up to the Terms of Offer, NHS Conditions of Contract. See Appendix A for section 35 of the NHS Conditions of Contract for the Supply of Services

4.2 Reporting of Information Security Events by Service Providers and Business Partner Organisations

Information security incidents should be reported to Warrington and Halton Hospitals NHS Foundation Trust and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur.

Definition of an Information Security Event

Incidents of theft, accidental loss or inappropriate disclosure of Warrington and Halton Hospitals Foundation Trust data should be reported to the relevant Information Asset Owner at the Trust. Procedural failure of equipment containing WHH data should also be reported to the Information Asset Owner responsible for the data.

How Information Security Events Need to Be Reported

In the first instance information security incidents should be reported to the Trust's IT Helpdesk 01925 662346. The incident will be dealt with in line with procedures contained within the Trust's Information Security Management System and its Information Risk Policy.

4.3 Physical Access

The following list contains trusted companies which will be allowed unsupervised access to the communication cabinets and server rooms.

Company Name	Responsible For	Contact information	Operational Hours
Esteem	Server Support	01937 861 008	24/7
Intrinsic Technologies	Network Support	0870 880 2791	24/7
DELL	SAN Support	0207 026 0021	24/7
BT	Gigabit Line/N3 Support	0800 085 0503	24/7
NTL	Gigabit Line Support	0800 052 0800	24/7
Nviron	Server/Medicorr Support	0845 270 4031	8an-5pm/Mon-Fri
Hunters	Cabling	0151 328 1234	8an-5pm/Mon-Fri
GE	PACS Hardware	0844 406 8000	24/7

Contractors working on behalf of the Estates department, during normal working hours all contractors sign in and out at the Estates Department and also sign for any keys issued. Out of hours, contractors would only attend site at the request of the on-call Estates Officer and, depending on the circumstances, they may be accompanied by a member of the Estates staff or, if not, would have to sign for keys at either Warrington Switchboard or at Halton Porters Lodge.

4.4 Network Access

Third party contractors may be given access to the Trust's network see 4.1 Non-Disclosure Agreement.

4.5 Software Amendments

In the event that software needs to be accessed for maintenance or testing by a third party, the companies shall be subject to the Terms of Offer, NHS Conditions of Contract. See Appendix A for section 35 of the NHS Conditions of Contract for the Supply of Services

5. Cleaning Services

Domestic Services clean all areas of the Trust. They are permitted access to the following areas only:

- The IM&T offices on the Warrington and Halton sites only.

The cleaning staff do not have permission to enter the server room or communications cabinets, it is the responsibility of IM&T and Estates staff to ensure the server room is kept in a presentable and safe state.

This includes but is not limited to:

- Disposing of boxes/packaging from hardware/software.
- Ensuring food and drinks are not taken into the server room.
- Ensuring books/manuals and documentation are filed and locked away after use.

6. Compliance

6.1 Responsibility

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

6.2 Review and Monitoring

Warrington and Halton Hospitals NHS Foundation Trust Trust has in place routines to regularly audit compliance with this and other standards.

Appendix A
Section 35 of the NHS Conditions of Contract for the Supply of Services

35. Confidentiality

35.1 In respect of any Confidential Information it may receive from the other party ("the Discloser") and subject always to the remainder of this Clause 35, each party ("the Recipient") undertakes to keep secret and strictly confidential and shall not disclose any such Confidential Information to any third party, without the Discloser's prior written consent provided that:

35.1.1 The Recipient shall not be prevented from using any general knowledge, experience or skills which were in its possession prior to the commencement of the Contract;

35.1.2 The provisions of this Clause 35 shall not apply to any Confidential Information which:-

(a) is in or enters the public domain other than by breach of the Contract or other act or omissions of the Recipient;
(b) is obtained by a third party who is lawfully authorised to disclose such information; or
(c) is authorised for release by the prior written consent of the Discloser; or
(d) the disclosure of which is required to ensure the compliance of the Authority or (as the case may be) any Beneficiary with the Freedom of Information Act 2000 (the FOIA).