Walton Centre

Asset Management

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
06/01/2004	1.1	L Wyatt	Addition of storage media
16/03/2005	1.2	Liam Wyatt	Update storage media in introduction and update to hardware / software support list

Table of Contents

Section	Contents
1	Introduction
2	Responsibilities within this Standard
3	Maintain an Inventory
3.1	Asset Inventories
3.2	Hardware Inventory
3.3	Component Data Notebook/PC/Server
4	Asset Maintenance
4.1	Inventories
4.2	Removal, Re-use and Disposal of Assets
4.3	Software Licensing
5	Asset Classification
5.1	Principles
5.2	Classification Scheme
6	Equipment Maintenance

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 Walton Centre. These standards, procedures and policies are used as part of the information security management system (ISMS) within The Walton Centre.

A mandatory requirement for BS7799 certification is to have a clear understanding of the information assets involved and to document these in an Information Asset Register.

The Information Asset Register also forms a key input to the Risk Assessment, another mandatory requirement for certification.

The purpose of this Information Asset Register is to identify the different types of information processed, stored and communicated by The Walton Centre. The Information Asset Register is essential to the Risk Assessment and for compliance with BS7799, because it is the foundation for the selection and deployment of security controls.

This Information Asset Register includes all information assets relevant to the clients Information Security Management System (ISMS) and details the classification and ownership of each of the information assets.

It is important to ensure that the Information Asset Register is kept under control and updated as necessary. The Information Asset Register should be updated every time the details of one of the information assets are changed.

This document outlines the standards and procedures for the recording, control, auditing, and disposal of information assets. It also includes standards and procedures for change control and hardware updates.

An information asset can exist in several formats, both in terms of the physical media on which the data is stored and in terms of whether it is permanently or temporarily stored. This affects the security controls that may be applied as a result of the Risk Assessment, e.g. paper documents may be locked in a cabinet whilst files stored on a network drive may require setting of system access rights for protection.

The sub sections below detail each of these basic categories.

Paper

Much of the information exists in conventional paper form, although it is likely that originally it would have been produced on a computer. Also in this category are printouts of electronic documents, files and logs.

Electronic

This is data that is stored electronically, either within (*the client's*) equipment or on electronic media.

Data stored within the equipment is most commonly stored on an internal hard disk. Protection of this is ensured through the physical access to the machine and through the logical controls that are managed through the configuration of the operating system.

This data may be backed up or copied onto other media, including floppy disks, CD-ROMs/DVD's, tapes, USB devices and Pen Drives. These are protected through physical measures in a similar manner to paper documents. A summary of the media types is given below:

Floppy disk

These are 3.5-inch diskettes with a storage capacity of 1.44Mb readable by virtually any computer;

CD-ROM

These have a capacity of 650Mb and exist in two formats, CDR, which can be written to once and cannot be erased and CDRW, which can be rewritten in a similar manner to floppy disks;

DVD-ROM

These have a capacity of 4.7 Gb and exist in two formats DVDR which can be written to once and cannot be erased and DVDRW, which can be rewrited

Pen Drives/USB Drives

This are portable storage device's which can be rewritten as often as the user likes the size of the storage is up to 4gb and over depending on current technology.

Tape storage

Tape cartridges that require a specialist device to read and write data to. These can have various capacities, up to several Gbs.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

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

3. Maintain an Inventory

The document incorporates the following sections:

- Asset Inventories Procedures.
- Asset Maintenance Procedures.
- Software Licensing Procedures.

- Document Classification.

3.1 Asset Inventories

It is important that we standardise the hardware asset register, using an easy to read, and track naming convention.

Each hardware device will have an asset tag placed in a visible location, no tags should be placed over any existing serial numbers.

The asset tag should show example Insert detail

3.2 Hardware Inventory Registers

All hardware devices are entered onto an electronic asset register accessed only by staff within the Informatics Services Department. The following information will be collected relating to equipment purchased though the Informatics Services Department

- Manufacturer, product description and model/serial number.
- Any purchase/lease information where available, (details of lease agreement to be referenced).
- Owner of equipment.

3.3 Component Data PC/Notebook/Server

- Manufacturer, product description and model/serial number.
- Software installed, manufacturer, product and version.
- Configuration, Build.
- Business Owner.

4. Asset Maintenance

4.1 Inventories

All Asset registers must be reviewed every 3 months, but constantly updated when changes occur, by the IT Support Manager / Deputy Head of IT

A network audit can be carried out at any time using the Audit Wizard software can look at the following information

- Category (PC,Server,Printer)
- Make (Dell, Compaq ect)
- Model (Dell insparon)
- Hardware
    - Bios (Date, Manufacturer, Version)
    - Number of drives including letters (Type, Size, Label, Free Space)
    - Environment Strings
    - Graphics (Adapter, Colour Depth, Monitor, Resolution)
    - Memory (Type, Size, Number, Capacity)
    - Motherboard (Processor, Bus type, Co-processor, Speed, Sockets, Voltage)
    - Network (IP Address, Logon Client, MAC Address, Network Adapter, Protocols, User Name)
    - Peripherals (All attached peripherals)
    - Sound, Video and Games Controllers
    - USB (All Devices)
- User information
- Software installed (licences)

The software can also check internet history and cookies installed on the machine

Software audits and spot checks maybe periodically be carried out at any time.

Asset tags must verify the identical information in accordance with the Asset register; any missing or damaged tag must be replaced immediately. If any part of the asset register does not match the piece of hardware/software/data then changes should be made and recorded.

Any unlicensed software identified will be removed immediately, and cannot be reinstalled until a license is purchased.

4.2 Removal, Re-use and Disposal of Assets

Any equipment considered out of date, redundant or inoperable, beyond cost effective repair will be dealt with in the following manner.

The IT department must be consulted when any piece of equipment is deemed to be obsolete or redundant, so they can make the decision as to whether it can be used else where within the company. This must be done prior to its removal.

If no alternative use has been identified, then the piece of equipment must be completely sanitised, including the destruction of disks prior to disposal. All asset tags shall be removed and the relevant register amended.

The following company has been authorised to dispose of equipment in a safe manner

Insert detail

Media shall be disposed of in a manner appropriate to the media concerned. This shall comprise:-

- **HARD DISKS** - by means of degaussing to remove data
- **FLOPPY DISKS, TAPES and CD'S** – by physical destruction under guidance of IT
- **Documentation** – by shredding

4.3 Software Licensing

The majority of software used by The Walton Centre is covered by corporate license agreements with the vendors, or under natural license agreements.

It is the responsibility of IT Systems Manager to ensure that The Walton Centre has the correct numbers of licenses for software that has no agreement in place.

All licenses are kept by IT Systems Manager in the filling system setup as part of the Informatics Services Department documentation.

Under no circumstances must employees download or bring in unlicensed software, if there is a requirement to test new software, it must first be installed in a staged environment, and once approval has been granted by IT Systems Manager, he/she must ensure that adequate licenses are purchased to support the Company's needs.

5. Asset Classification

5.1 Principles

Information assets represent a valuable resource to the organisation and as such require protection. However, the information held and used by the organisations varies greatly in its value and as such it may be treated with equally varying degrees of security. In order for this to be workable it is necessary to establish a clear classification scheme to apply to all information. This classification scheme, allied to removal, disposal, handling procedures etc will provide guidance to staff in the effective management of information.

It is the responsibility of all employees to ensure that all data created, stored or used by them have the correct classification associated with it. If documents fall into the restricted or confidential categories then it is your responsibility to ensure it is labelled and handled correctly.

5.2 Classification Scheme

The NHS does not current use, nor does it advocate, any form of information classification. Given the cross organisational delivery of patient care it is not appropriate for individual organisation to develop a classification in isolation of its potential care partners.

Work is being undertaken at national level to develop an NHS wide scheme which will be adopted by the Trust in due course.

6. Equipment Maintenance

One threat to the Trust's computer-based systems (& hence its business continuity) is that of equipment breakdown or failure. To overcome this, an equipment maintenance strategy has been developed. The servers and other equipment are, generally, extremely reliable so it is not necessary to have regular, planned maintenance carried out by manufacturers' engineers. The strategy adopted is a combination of built-in redundancy, call-out maintenance contracts and in-house repair – with equipment still under warranty being repaired or replaced by the supplier or manufacturer as required.

This section outlines the processes in place to maintain the Trusts equipment.

The following are contact details for all external support companies used by The Walton Centre to maintain all hardware and software

The first point of contact for all quires is the IM&T Help Desk ext Insert detail all calls will be logged then escalated if required;

Hardware

Hardware	Department Contact	Support Company	Contact information

Software

Software	Department Contact	IM&T contact	Company	Contact information

Software	Department Contact	IM&T contact	Company	Contact information