Walton Centre

Physical and Environmental Security

Document History

Date	Version	Author	Changes
01/10/04	1.0	A Cobain L Wyatt	
06/01/2005	1.1	L Wyatt	Update of Trust information
18/03/2005	1.2	Liam Wyatt	Update to procedure

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 Instruction Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

This procedure outlines how the Trust maintains a controlled working environment.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

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

3. Environmental Security

The Trust receives facilities management services that operate during normal business hours through a Service Level Agreement with the University Hospital Aintree. Details of an up to date version of the on call rota can be found on the public folders under senior manager's on call rota. Who ever is on call is contactable by pager on weekends and evenings in cases of emergencies

- Health and Safety is the responsibility of the individual and there line manager
- Employee Safety Assurance
- Access Control (A member of security will be available to deal with any quires regarding access control and the issuing of keys 24 hours a day)
- Issuing of keys and photo identification
- Emergency Response
- Business Continuity

4. Security and Access Control System

The Trust's security and access control system manages and monitors physical entry and personnel's movements, It is run on a PC.

This system enables us to gather information relating to:

- Date
- Time
- Valid Codes
- Access Levels

Access Control readers are strategically situated and programmed to restrict access to every entry point associated with the Trust's IT department.

Security incidents such as rejected cards, forced entry, doors wedged opened or not closed properly activate alerts and this information is also recorded for up to (*insert time period).*

The IT department and Server room have floor to ceiling partitions for protection.

4.1 Physical Security Policy

All personnel working for the Trust in the IT department will be approved to have full-unrestricted access to the Informatics Services Office, only the following will have access to enter the server room's or communications rooms

Insert detail

Each member of staff will be issued with a swipe card and a photo id containing credentials.

Any access required to unauthorised areas will be reviewed by one of the following people:

Insert detail

Once access has been granted to unauthorised parties, they must at all times be escorted around the restricted areas.

4.2 UPS System

If any of the following incidents occur, please inform IT Systems Manager, using the contact list at Section 4.

- A UPS fault occurs which will not clear.
- The battery status message indicates a discharging battery although the input power, rather than the battery, is supporting the load.
- Repeated start-up attempts are unsuccessful.
- Any indicators or alarms operating improperly.
- The normal operations of the critical load repeatedly cause an overload condition. Although this is not a UPS fault, a qualified person should analyse the total load connected to the UPS

- Any other abnormal function of the system occurs.

The UPS will be subject to monthly testing.

4.3 Air Condition

The air conditioning units are ceiling mounted, and for the office environment, there is a control thermostat available for use.

The air conditioning units for the server room have a preset temperature, which must not be adjusted unless prior permission is granted the Head of IT.

Should any air-conditioning unit become faulty please report this through the Trusts fault reporting mechanism ie IT helpdesk.

4.4 Generator

In the event of a power failure or when the power supply drops, there is a generator placed at the edge of The Walton Centre's staff car park opposite the Clinical Sciences Building which will provide the Trust with an electrical supply to *enable us to continue operations.*

Should a fault occur please report immediately to the shift engineer (Insert contact detail)

The generator will be subject to monthly testing.

4.5 Transfer Switch

There is a transfer switch installed which automates the transfer of a normal (UPS) power source to a standby (emergency generator) supply. It transfers from normal to standby within 30 seconds for none clinical areas and immediately for clinical areas

Should a fault occur please report immediately to the shift engineer (Insert contact detail)

The transfer switch will be subject to monthly testing.

4.6 Equipment Sitting and Protection

In accordance to the Health and Safety Act, the Trust has positioned all equipment with due consideration.

Consideration has also been given to the protection of information available from it.

Should any member of staff require the repositioning of equipment, permission must be obtained from the Informatics Services Department.

Network cabling, where possible, will be within the fabric of the building (i.e. in ducting and risers etc). Where this is not possible cabling will be within appropriate trunking.

All cables must be stored in cable trays or tied and secured in the office environment, no cables must be laid across open floors as these are hazardous and could cause an employee to trip. Any cables leaving the IT department must be protected against accidental or intentional damage.

It is the employee's responsibility to ensure that any computer equipment that has been provided to them solely for their use remains in the same condition as it was when released. Disciplinary action may be taken against personnel if any case of misuse against equipment is found.

It is the responsibility of every employee to report any fault to do with the infrastructure to the Estates so that a decision can be made as to whether the problem can be rectified internally, or whether it needs to be escalated.

Any security incidents, hardware or software failure must be documented and reported providing information of the status, even if the problem has already been fixed, so it can be reviewed accordingly.

5. Compliance

5.1 Responsibility

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

5.2 Review and Monitoring

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