Walton Centre

Access and Authentication (physical)

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
06/01/2005	1.1	L Wyatt	Update to procedure
31/03/2005	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 Instructions 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.

The Trust has implemented several countermeasures and checks to ensure integrity and confidentiality of its information and network devices. These Standards and Procedures outline the way in which we prevent unauthorised access to our assets physically.

This procedure establishes physical security for the Trust.

This document will include the following sections:

- Clear desk/screen procedure
- Laptop control procedure
- Physical Access controls for unauthorised parties
- Visitors procedures

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. General standards.

These Standards, Policies and Procedures are used as part of the Information Security Management System (ISMS) under the standards of the BS7799-2

All Trust IT staff will be given full access to the Informatics Services Office with only a number of staff with in the Informatics Services Department being granted access to the Server Rooms and Communications rooms.

Every employee will be given a full induction and access credentials (photo ID swipe card/pin number) to gain access to secured areas.

Access is gained through the rear of the building by the porters lodge using swipe access.

Non-Trust personnel enter the building though the main entrance and report to the reception area to sign the visitor's book and will be issued a visitors pass for the duration of there visit.

Non-Trust personnel will be given unescorted access to Communications rooms.

Non-Trust employees must be escorted at all times when going into secure areas.

Access to secure areas by maintenance personnel will be allowed as required. However these personnel must be closely escorted at all times.

To ensure accountability all non-Trust employees will be required to sign a visitor's book at the main reception and also when entering the server rooms.

3.1 Review

These standards and procedures will be reviewed at intervals of not more than one year. In response to any serious security incident or business change affecting the original risk assessment on which these standards and procedures are based, a recommendation will be made and new procedure incorporated.

3.2 Clear Desk/Screen Procedures

Clear Desk and Screen Policy

Due to the confidential nature of the work that can be carried out by the Informatics Services Department The Walton Centre supports a clear desk policy.

At the end of each the working day, all documentation and files must be placed back on the relevant book shelf or filling cabinet. Each desk should be equipped with a set of stacker trays for non confidential information. Desks should be free from clutter with the exception of books and manuals.

All staff must either lock or log off their computer at the end of the day or when leaving the office.

This procedure is put in place to enable us to protect against unauthorised personnel from being able to view or download business information, whether physically or electronically.

3.3 Physical Data

All desk and workstation areas must be kept clear and in an organised condition at all times.

As soon as documents have been finished with, they must be filed.

If business information is no longer required, then these must be destroyed by means of shredding. Ensure documents have been shredded before leaving the shredding machine.

3.4 Electronic Data

Software must be signed out if needed.

Under no circumstances must unauthorised firmware or software be used. However it may be used for testing purposes within the Informatics Services Department.

Employees must ensure they log off when leaving their machines, rendering the computer unusable and denying any unauthorised personnel access to our systems.

Screensaver passwords must be set to activate after 10 minutes of no activity is detected to ensure no unauthorised personnel can gain access to our systems.

3.5 Control Procedures for Laptops

The Informatics Services Department will only take responsibility and control for laptops used by staff within the department and laptops that leant out to users.

- Laptops are restricted to a small number of staff within the Informatics Services Department. To gain access to a laptop the user must have a relevant user name and password and are not to store trust sensitive information on them.
- The use of laptops by other Trust staff is permitted to any member of the Trust and it is down to the responsibility of the person borrowing the laptop to ensure its safety and security.

3.5.1 Data Security procedure

Access to the file system will be managed through the NTFS file system.

Remote communication will be through a secured RAS using two factor authentication.

Data access levels will be controlled through the OS.

Employees must ensure when leaving their machines for any length of time that the computer is locked, thus denying any unauthorised personnel access to our systems.

Screensaver passwords must be set to activate after 10 minutes of no activity to ensure unauthorised personnel cannot gain access to our systems.

3.5.2 Physical Security Procedure

When working in the office, laptops must be secured to a docking station, were possible.

If you are away from your desk for considerable lengths of time, the laptop must have the network account locked and were possible the laptop secured.

Employees who use laptops should always be aware of unauthorised parties who maybe shoulder surfing.

Employees are responsible for their assigned laptops; at the end of each day they may lock them away in a lockable drawer or cabinet if provided. The Informatics Services Department is considered a secure room with the following;

- Swipe card access.
- Key code access (when office is un manned).
- Conventional lock for out of hours.

Consideration must be given when transporting the laptop around, i.e. place the laptop in the boot of the car whilst in transit; you would also be expected to take it inside the house rather than leaving it in the car.

3.6 Security Controls to Protect against Unauthorised Access

3.6.1 Physical Access (External)

CCTV monitoring the doors controls physical access to the building as The Walton Centre is a public building. The doors to none public areas have swipe card access some areas also require control pads that require a pin number to be entered, this number must not be communicated to any unauthorised party. (Employees should be aware of shoulder surfers when keying in the passwords and numbers.)

Any breach in this procedure should be reported immediately, and treated as a security incident, so that countermeasures can be put in place straight away.

Any defects, such as doors not being secure or wedged open should also be reported.

3.6.2 Physical Access (Internal)

The Trust's internal access is protected by a swipe cards for none public areas, with some areas requiring additional keypad access, in which only authorised personnel are given the number; under no circumstances should this number be supplied to any unauthorised personnel.

Any breach in this procedure will result in a security incident, and must be reported immediately, It is also expected that employees noticing any defects i.e. a window not closing would report it immediately.

3.6.3 Name Badges

All employees and contractors will be supplied with a name badge; these are of a distinctive design incorporating the employee's photo and name and must be worn at all times. Any loss or damage to these cards must be reported immediately and will be treated as a security incident.

It is the responsibility of every employee of The Walton Centre to question anyone who is in a restricted area without a name badge, and to report this as a security incident.

3.6.4 Equipment

Access to any equipment on the Trust site by non-Trust employees, is allowed only upon written confirmation from the Head of IT or Information Security Officer.

Removal of equipment from the Trust is only permitted with written permission from Head of IT, and this should be done in accordance with the Asset Management and Control procedure.

3.6.5 Visitors Sign-In procedure

All visitors must report to reception on arrival where they will be required to fill in a visitors book, the information required to be completed are as follows:

- Name
- Company
- Person Visiting
- Car Registration (if applicable)
- Date
- Time In

All this information needs to be completed in block capitals.

The reception area will then contact the person being visited, who will in turn come and collect their visitor from reception.

All visitors must wear their visitors name badge at all times, visitors must sign out when leaving the premises, and complete the time out section.

If accessing the server room visitors must state why they need access and date and sign in the visitors log book in the server room.

4. Compliance

4.1 Responsibility

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

4.2 Review and Monitoring

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