Walton Centre

Information Security Management Policy

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain Liam Wyatt	
15/03/2005	1.1	Liam Wyatt	Version control and update scope of point 6.2

Table of Contents

1. Introduction

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

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

These objectives of this policy are:

- Provide a corporate framework in which security threats to our Information Systems can be identified and managed
- Illustrate Management's commitment to the security information and information systems.
- Provide accepted laid down procedures that ensure uniform security implementation.

By putting procedures in place the risk from unauthorized modification, destruction or disclosure of information, whether accidental or deliberate will be minimal. This can only be achieved if everyone observes the highest standards of personal, ethical and professional conduct.

2. Approval

This policy is approved and signed by (*name and title of person)*.

Chief Executive: ……

Date: ……

3. Responsibilities Within This Policy

Particular responsibilities within the policy are defined as:-

Review and Maintenance	Information Security Officer
Approval	Trust Board
Local adoption	All managers, staff and contractors

4. Definitions

This document links into the Trust information security management system (ISMS). The ISMS deals with the process of ensuring the integrity, confidentiality and availability of an organisation's information assets, whether these are held electronically, as a hard copy, or from memory. Integrity means ensuring the accuracy and completeness of any information held or processed. Confidentiality means ensuring that information is available only to those that need to have access to it. Availability means ensuring that those who need it are able to access information at the time it is required.

5. Intent

The Trust acknowledges that information is a valuable asset, therefore it is wholly in it's interest to ensure that the information it holds, in whatever form, is suitably protected from any threat. The Trust acknowledges that, by doing so, it will act in the best interests of its, employees and all third parties to whom the information is shared with. Protecting the intelligence ensures minimised business damage and business continuity. This document constitutes an Information Security Management Policy, as required under section 3.2 of BS 7799-2: 1999.

6. Operating Procedures and standards

6.1 Compliance

It is the policy of the Trust to ensure compliance, in accordance with all the legislative obligations. The Trust also requires all employees, contractors and third parties to comply with this policy and supporting standards and procedures where appropriate. Procedures for relationship with third parties are contained in section SS 05 Third Party Relationship.

6.2 Security Awareness and Education

It is the responsibility of all employee's and third party's of the Trust to sustain excellent information security. To comply with this, the Trust requires that all employees and contractors within scope to understand the importance of information security and are familiar with this document, and supporting documents where appropriate.

6.3 E-Mail and Electronic Systems

The Trust has clear standards relating to the use of e-mail, Internet and intranet and the deliberate or accidental misuse of electronic systems. The procedures cover use of any systems used to store, retrieve, manipulate and communicate information (e.g. telephone, fax, e-mail, IT systems and the Internet). These standards are laid out in SS 09 Email and Internet and all employees and third parties are required to familiarise and adhere to them.

6.4 Access

The Trust has a procedure outlining the control of access to its premises, physical assets and electronic networks. Procedures also cover correct use of its assets. All employees and third parties are required to acquaint themselves with these standards (*see Sections numbered*).

6.5 Physical and Environment Security

The Trust has clear procedures outlining the physical protection of its information assets from loss or damage, however caused. All employees and third parties are required to acquaint themselves with these standards (*see Sections numbered*).

6.6 Personnel Security

The Trust has clear procedures outlining the compromise of its information assets through deliberate actions by its employees. All employees and third parties are required to acquaint themselves with these standards (*see Sections numbered*).

6.7 Business Continuity

The Trust recognises that continued access of information is vital to its business. It therefore has a policy of ensuring business continuity in the event of serious disruption, damage or disaster to its information management systems. It is the responsibility of all employees and contractors to familiarise themselves, as appropriate, with the business continuity plan that supports this policy (*see Section number).*

6.8 Violations

It is a condition of employment with the Trust that compliance should be maintained where appropriate with the information security management policy, and supporting standards and procedures. If any procedures or policies are violated these must be treated as security incidents, and reported in accordance with the secure responsibilities operating procedures. Failure to comply with this policy, or supporting procedures, could result in disciplinary action being taken against the employee in accordance within security standard SS02: Personnel Security.

7. Review

This policy will be reviewed annually, and in response to any serious security incident or business change affecting the original risk assessment on which this policy is based.

8. Supporting documents and procedures

The documents which support this security are as set out within the contents page of the Information Security Management System (Ref CON 01: Table of Contents)