Walton Centre

Monitoring & Audit

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	

Table of Contents

1. Introduction

Information and information systems are important 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 Walton Centre

The Walton Centre acknowledges that we must demonstrate to our stakeholders our commitment to, and delivery of, effective information governance.

The aim of The Walton Centre's Security Policy, Standards is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within The Walton Centre. These policies, standards, guidelines are used as part of the information security management system within The Walton Centre.

The Walton Centre places great reliance upon the robust application of the policies and standards that make up the ISMS and has, therefore, developed processes to self assess compliance and for independent review, by its internal auditors.

This standard applies to all staff, whether permanent, part-time or temporary with responsibilities defined below.

2. Responsibilities Within This Standard

All employees using IT equipment, the internet or e-mail have responsibilities with regard to 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. Monitoring

3.1 Context

Auditing, by its nature, is based on samples and random checks and, while providing valuable assurances to the Board, it does not take away the Trust's responsibility to self manage, ensuring compliance with its Information Security Management System as well as legal and regulatory requirements (examples of applicable legislation are included within the ISMS's Incident Reporting Standard).

To this end the Trust reserves the right to monitor the activity of individual in appropriate circumstances acknowledging the legal requirements and restraints applicable.

In determining the need for and appropriateness of monitoring due reference has been made to the Information Commissioner's Monitoring at Work Guidance, The Human Rights Act and the Regulation of Investigatory Powers Act.

In particular, the Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the Trust's business, and the employees position with the Trust.

3.2 Impact Assessment

Having due regard to the sensitivities related to patient and Trust information and the need to demonstrate to the public our determined efforts to ensure effective information governance it the opinion of the Trust that it is appropriate that it retain s the right to monitor information flows within as well as into and out of the Trust.

The Trust is aware that monitoring is a sensitive issue and it seeks to minimise any adverse impacts through effective consultation and communication with staff. All of the Trust's Information Security Standards will reflect the right to monitor and these rights will also be included within contracts of employments and confidentiality undertakings.

3.3 Examples of monitoring

While not intended to be exhaustive or all inclusive, the list below provides examples of the monitoring which the Trust does or may wish to undertake:-

- Examining logs of web sites visited to ensure appropriateness
- Using internet filtering software to block and report on inappropriate internet access attempts
- Scanning of e-mail for inappropriate content
- Randomly opening e-mails or listening to voice-mails for evidence of inappropriate practice
- Monitoring of telephone logs for evidence of inappropriate contacts e.g. premium rate numbers
- Use of CCTV (closed circuit television) to ensure no breach of standards.

While a number of the above, e.g. internet logs, internet filtering and e-mail scanning, may be routinely in place others may be invoked as and when a concern of needs arises.

4. Internal Audit

4.1. Policy Statement

It is the policy of the Trust that all aspects of the its Information Security Management System (ISMS), be subject to an internal review at least once every 12 months. This will help ensure that not only policies and procedures are being applied but that new best practice can be gathered and applied.

4.2 Process

4.2.1 Overview

This audit process is undertaken by Trust staff and is distinct to audit work undertaken by its internal auditors. It is undertaken in discussion with staff members in the area under review, identifying whether existing procedures are complied with and at the same time identifying whether the procedures are adequate. This will involve observing work in progress as well as sampling previous records. The auditor(s) will also gauge overall security awareness of the staff members interviewed.

Audit Checklists will be used, an for guidance only and will not limit the enquiries of an auditor who is following the audit trail. In addition the Audit Checklists may be used to record relevant information during the course of the audit.

4.2.2 Reporting Audit Findings

Findings will be recorded and subsequently will be classified by the auditor, as either a recommendation or as an observation. This will be recorded on an audit finding form. (See Appendix B) and summarized on the audit summary form (See appendix C)

The Auditor will ensure that each recommendation has a unique identification number (the audit number followed by a second sequential number). This information will be added to the Internal Audit log. The Department Manager will sign to accept the recommendation.

At the end of the audit the Auditor will generate an Audit Report (template at Appendix D). This Report will consist of any Audit Checklists and notes, copies of any observations, copies of any recommendations, if applicable, a summary of the audit findings and a front page. The front page will detail the Area/Function audited, the unique audit number, the date and time the audit was carried out, the auditor(s), auditee(s) and a list of attachments.

An urgent 'Recommendation' indicates that an aspect of the ISMS is either not defined or not being adhered to in any way and hence a risk to the business. Such a recommendation would need to be addressed as a matter of urgency.

The Auditor may also see fit to raise an 'Observation' which is not a firm recommendation but rather a suggestion for improvement. Upon the next visit, the Auditor will expect the 'observation' to have been taken on board (if appropriate) thus signifying ongoing improvement to the ISMS. Any non-site specific observations will be shared with other sites.

4.2.3 Following Up Corrective Actions

Once the Information Security Officer has received the completed non-conformities the Audit Summary From is then updated to show when follow up review is required.

The purpose of this verification (follow up) audit is to ensure that the defined corrective actions have been successfully implemented and are effective. The auditor who raised the original recommendation normally conducts this audit.

Once objective evidence has been found confirming the successful implementation and effectiveness of the actions, the recommendation will be closed and signed off by the auditor and the department representative. The Information Security Officer will review the recommendation and authorise its closure.

5. External Assurance

The Walton Centre senior managers and board require, in order to meets it corporate governance and NHS reporting requirements, independent assurance that its information security processes are robust and that the policies, standards and procedures are appropriate to business need. In simple terms these requirements can be described thus :-

Adequacy	This process would aim to ensure that policies, standards and procedures are fit for purpose in their design.
Effectiveness	At this level audit work would aim to provide assurance that such policies, standards and procedures have been robustly and effectively applied within The Walton Centre

In order to ensure that The Walton Centre board can obtain appropriate assurances it is essential that sufficient audit resources are assigned to the review process. On an annual basis the Director of Finance, in conjunction with the Internal Audit function will assess the assurance requirements for the following year and will allocate appropriate time within the internal audit plan.

Reports by the internal audit function which related to information security will, initially be reported to the Head of IT and the Director of Finance. They will subsequently be issued to the Information Security Forum, where appropriate, for action.

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

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

APPENDIX A: SCHEDULE OF INTERNAL ISMS AUDITS

ISMS Section	Document Title • Risk Management Schedule reference	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR
ISMS 01	Information Security Management Policy • Security Policy	X						X					
ISMS 04	Asset Inventory		X						X				
ISMS 05	Risk Assessment / Risk Management Plan			X							X		
ISMS 06	Business Continuity Plan • Recovery Options for Hosts • Recovery Options for Network Interfaces • Recovery Options for Network Services • Recovery Options for Accommodation • Recovery Options for Media • Network Resilience • Equipment Failure Protection						X						X
ISMS 07	Document Control	X						X					
SS 01	Security Responsibilities • Security Education & Training • Security Infrastructure	X						X					
SS 02	Personnel Security • Personnel						X						
SS 03	Asset Management • Object Re-use • Hardware Maintenance Controls • Software Maintenance Controls • Document / Media Controls		X						X				
SS 04	Risk Assessment			X							X		
SS 05	Third Party Relationships			X									

ISMS Section	Document Title • Risk Management Schedule reference	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR
SS 06	Physical and Environmental • Room / Zone Physical Security • Physical Network Protection • Theft Protection • Physical Equipment Protection • Fire Protection • Water Protection • Natural Disaster Protection • Environmental Protection						X						
SS 07	Access and Authentication (Physical)						X						
SS 08	Access and Authentication (Network) • Identification & Authentication • Logical Access Control • Software Integrity • Customer Authorisation • Network Access Controls •						X						
SS 09	Acceptable Use • Content Scanning • Anti-spamming Controls							X					
SS 10	Encryption								X				
SS 11	Change Control • Security Testing • Software Change Control • System Administration Controls • Hardware Maintenance Controls • Software Maintenance Controls		X						X				
SS 12a	Incident Reporting										X		
SS 12b	Incident Response (Legal & Forensics)										X		
SS 12c	Incident Response (Operational)										X		

ISMS Section	Document Title • Risk Management Schedule reference	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	JAN	FEB	MAR
SS 13	Anti Virus and Housekeeping • Protection Against Malicious Software • Mobile Code Protection • Back-up of Data			X									
SS 14	Remote Working • Mobile Computing & Teleworking											X	
SS 15	Network Management • Accounting • Audit • Network Security Management • Vulnerability Analysis • Intrusion Detection • Quality of Network Services • Operations Controls • User Control • Capacity Planning											X	
SS 16	Business Continuity • Business Continuity Planning						X						X
SS 17	Monitoring & Audit											X	
SS 18	Communications • Security of Routing Tables • Wireless LAN Security • Message Security • Protection Against DoS Attacks • Data Integrity Over Networks												X

APPENDIX B: AUDIT FINDING FORM

AUDIT REF	
AREA	
FINDING No	

DATE	
AUDITOR	

FINDING / OBSERVATION (delete as appropriate)	PRIORITY: NORMAL / URGENT

ACTION REQUIRED

ACTION BY (officer)	
ACTION DATE	
SIGNED BY AUDITEE	

FOLLOW UP

CLOSED BY	
CLOSED DATE	
SIGNED BY AUDITOR	

APPENDIX C: AUDIT SUMMARY FORM

AUDIT REF		DATE	
AREA		AUDITOR	

FINDING NO	AUDITEE	ACTION DATE	FOLLOWED UP DATE	CLOSED DATE

APPENDIX D: AUDIT REPORT TEMPLATE

ISMS Audit Report

Auditor:	[Click **here** and type name]
Date:	[Click **here** and type name]
Audit Area:	[Click **here** and type name]
Audit Ref:	[Click **here** and type name]

1. Scope and Objective

The audit undertaken aimed to assess the Trust's compliance with its internal Information Security Management System and thus with the requirements of BS7799.

This particular review focused on the following elements of the ISMS:-

- Xxx
- Xxx

2. Summary of Findings / Observations

The audit identified xx non-conformances of which xx were considered to be of an urgent nature. These findings are summarised below:-

FINDING REF	ISSUE

In addition, there were xx observation raised which are summarised below:-

FINDING REF	ISSUE

3. Conclusion / Opinion

Having assessed the findings arising from the review it is apparent that the ISMS *has / has not (delete)* been consistently applied and that *there is on-going compliance with the requirements of BS7799 / compliance with BS7799 cannot be assured.*