Walton Centre

Security responsibilities

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
15/03/2005	1.1	Liam Wyatt	Update to Trust information point 2

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, Standards and Procedures 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 purpose of this procedure is to outline the roles and responsibilities for managing security (as in the ISMS), security incidents and controls.

2. Information Security Management Responsibilities

Responsibility for managing information security within the Trust's rests with all employees and the following people in particular:-

- Insert details

2.1 Head of Information Technology

The Head of IT will be appointed by and report to the Director of finance.

The Head of IT will have overall responsibility for the Information Security Policy, operating procedures, processes and their adherence; he/she will also be responsible for the review of the ISMS and accompanying documents.

The Information Security Forum provides assistance.

2.2 Information Governance & Security Forum

The Trust has established a cross functional Information Governance Security Forum to promote and monitor information security as an aid to the delivery of high quality healthcare.

The Forum will maintain a focus on the scope of the ISMS but will also take a wider view of information security across the Trust in order that good practice etc can be disseminated and developed in all information related activities.

The Terms of Reference of the Forum are as set out at Appendix B.

2.3 Implementation Manager

The Implementation Manager will act in the capacity of Information Security Officer and will have day to day responsibility for review and maintenance of the Information Security Management System

2.4 Reporting Structure

Insert details

3. Roles and Responsibilities

3.1 The Trust

The Trust is responsible for ensuring that all staff are providing with appropriate training and education in order to allow them to discharge their security responsibilities.

3.2 Information Governance & Security Forum

The Information Governance & Security Forum is responsible for those activities set out within its Terms of Reference as detailed at **Appendix B**.

3.3 Manager(s)

The line manager(s) responsibilities are:

- Ensuring they are aware of the Trusts Information Security Management System (ISMS)
- Making sure their staff are aware and comply to the ISMS
- Ensuring countermeasures are discussed and implemented in conjunction with security incidents after consultation with the ISGF
- Reporting security incidents to the Information Security Forum (ISGF), and ensuring that the reports are fully documented including type of incident and countermeasures put in place. They must be submitted to the Secretary of the ISGF

- To attend regular ISGF meetings in which security incidents relating to his/her department along with other security incidents are discussed, resulting in action plans being created and distributed to the relevant managers.
- Initiating the necessary disciplinary action if a member of staff is found to be disregarding procedures which could result in a security incident
- Liasing with senior management and HR if incidents occur, which may result in termination of employment.

3.4 Implementation Manager / Information Security Officer

The Information Security Officer's (ISO) responsibilities are:

- To arrange meetings on behalf on the ISF which include:
  - Booking a venue
  - Arranging time and date
  - Sending out invites
  - Producing an agenda
- Taking minutes and distributing them to members and attendees of the ISF
- Ensuring that security incidents submitted are documented with all the required information
- Document control for the ISMS and supporting documentation

3.5 Employees

The employee is responsible for:

- Making themselves aware of the ISMS and the relating documentation

- Making sure they adhere to the ISMS
- Highlighting any areas of inappropriateness or ineffectiveness in operating procedures to their line manager
- Reporting security incidents to the relevant people. (See appendix A for contact details)
- Immediately reacting to security incidents and escalating to the appropriate people
- Informing your line manager of any colleague's behaviour that may result in a security incident.

Appendix A: Contact list

Physical and Environmental contacts

For physical or environmental security incident please contact one of the following people.

Name	Direct line	Mobile/Pager

HR contacts

For personnel incidents please contact one of the following people.

Name	Direct Line	Mobile/Pager

Network contacts

For network security, incidents please contact one of the following people.

Name	Direct Line	Mobile/Pager

Note: Any employee who raises a security incident must ensure that they fill in a security incident report immediately.

Appendix B: Information Governance & Security Forum – Terms of Reference

Table of Contents

1. Introduction

This document sets out Terms of reference for the Information Governance & Security Forum

Information Security can be defined as :-

"The development, delivery and management of a secure network infrastructure within the Walton Centre NHS Trust"

Information Governance is encompassed in four fundamental aims:-

- To support the provision of high quality care by promoting the effective and appropriate use of information.
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

2. Constitution:

The Board hereby resolves to establish a Committee of the CPSC to be known as the Information Governance & Security Forum (IGSF).

3. Membership:

- Director of Service Delivery & Performance (Chair)
- Head of IT
- Implementation Manager (Information Security Officer)
- Medical Director (Caldicott Guardian)
- Security officer
- Deputy Director of Nursing
- Clinical Risk Manager

- Medical Records Manager
- Head of Information
- PAS & Data Quality Manager
- Head of Health Care Governance
- Mersey Internal Audit
- Corporate Services Manager

4. Quorum:

5 to include or a representative:

- Director of Service Delivery & Performance (Chair)
- Head of IT
- Implementation Manager (Information Security Officer)

or any of the following:

- Medical Director (Caldicott Guardian).
- Security officer.
- Deputy Director of Nursing.
- Clinical Risk Manager.
- Medical Records Manager.
- Head of Information.
- PAS & Data Quality Manager.
- Head of Health Care Governance.
- Mersey Internal Audit.
- Corporate Services Manager

5. Authority:

To promote and monitor information governance & security as an aid to the delivery of effective healthcare

6. Attendance:

Members should attend at least six meetings per year

7. Frequency of Meetings:

The Committee will meet the last Friday of every month

8. Duties/Responsibilities:

The IGSF will be responsible for,

- The promotion of information security throughout the Trust information in all formats, written electronic, fax, spoken word.
- The review and recommendation for approval of all information security related policies and procedures
- The monitoring of progress in programmes to achieve certification
- The review and monitoring for the compliance, with standards and policies, and to monitor Information security incidents their cause and future prevention.
- Reviewing information security risk assessments and improvement plans.
- Receiving and reviewing information security related reports (e.g. internal audit)
- Reviewing and commenting upon the security impact of information system development.

- To support Information Governance & Security initiatives that promote best practice in the ten areas covered:-
    - Caldicott
    - Confidentiality Code of Practice
    - IM&T Controls Assurance
    - Records Management Controls Assurance
    - Data Protection
    - Freedom of Information
    - Health Records
    - IG Management
    - Information Quality Assurance
    - Information Security
- To monitor the performance of the Trust against national targets for Information Governance.
- To review and update Trust policies in respect of Information governance.

9. Reporting:

To CPSC / Trust Board