

Walton Centre

Network Monitoring

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
07/01/2005	1.1	L Wyatt	Update to procedure

Table of Contents

Section	Contents
1	Introduction
2	Responsibilities within this Standard
3	Network Management
3.1	Network Security
4	Internal Management
4.1	System and Security
4.2	Capacity planning
5	Clock Synchronisation
6	Compliance
6.1	Responsibility
6.2	Review and Monitoring

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.

It is important that the Trust monitor its internal network. Regular surveillance of our internal networks will ensure continued confidentiality, and allows us to review and put in place countermeasures to secure our networks. It also permits us to test best practice procedures.

This procedure outlines the way in which we monitor the company network.

This document will include the following sections:

- Monitoring the Network Perimeter
- Monitoring the Internal Network

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. Network Management

3.1 Network Security

The network administrator has implemented a network management and monitoring system, which will allow the Trust the ability to manage the network and its hardware remotely and monitoring performance, connectivity and integrity. This system is capable of maintaining a log of activities and those to be logged are detailed SS08: Access & Authentication

The network will further be protected by an appropriately placed and managed firewall. This firewall must have a contingency plan in place in case of failure.

4. Internal Monitoring

4.1 System and security logs

IT Support Manager is to check logs on an adhoc basis as they are detected and report any incidents of a security nature to the Information Security Officer. They are to be particularly vigilant in looking for traces of actual or attempted intrusion and for any internal user actions, which seem inappropriate. A form of sentinel software is to be run which looks at the veracity of selected files and reports accordingly. This will be checked daily.

Logs will be kept per the schedule with SS08: Access & Authentication

4.2 Capacity planning

Traffic and storage across and within the network is subject to regular monitoring in order to ensure that capacity and performance is appropriate to Trust requirements both now and in the short to medium term.

During system procurement and / or development the demands on traffic and storage will also be reviewed in order to ensure that these requirements are built into developments at the planning stage.

5. Clock Synchronisation

It is vital that information stored on our systems is assured validation of the actual time and date.

We do this by setting the servers up to a recognised time/date stamping service, and then all workstations are fed from these servers ensuring the correct time/date are displayed.

It is the responsibility of the IT Support Manager to ensure this procedure is carried out.

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.