Walton Centre

Anti Virus and Housekeeping

Document History

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

This document will include the following sections:

- Anti-virus procedures.
- Housekeeping

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. Anti Virus procedure

Viruses including Trojans and worms are among the most common forms of attack facing electronic communication. To enable the Trust to reduce the risks of such threats, and minimise the effects of the attacks, it is important our systems remain as virus free as possible, this procedure highlights the necessary steps required to help us achieve this.

Every desktop and laptop will have the company's approved anti-virus software installed on it before the computers are rolled out to employees.

The anti-virus software package itself is installed automatically when a user log onto a new PC. Consequently the definitions are pushed as a new definition/engine becomes available from the local antivirus central server. The central server itself updates definitions and engines hourly.

The anti-virus software must not be disabled or uninstalled at anytime unless a systems administrator has granted permission.

No software must be loaded on to computers at anytime, unless permission is granted from a systems administrator. Once permission has been granted the change management procedure must be followed.

Any data/software obtained from 3rd parties via floppy, cd or any others means, must ensure that it has been virus checked before placing the information onto the network.

Any data/software downloaded from the Internet or through email must make sure it has been virus checked before it is used.

3.1 User Responsibilities

Users should always remain vigilant and never open attachments from sources that are unknown to them. Remembering that the contents can be reviewed using the subject line without having to launch the attachment.

If you are in any doubt over the validity of a mail, then you should consult a systems administrator.

All employees should be alert to virus outbreaks; and ensure they are up to date with the latest virus software.

4. Housekeeping

This section contains the following:

- Information Backup
- System and Security Logs
- Fault Logging
- Operator Logs – Batch Processing
- Reporting System Failures

4.1 Information Backup

IT Support Manager is to ensure that all systems are backed up and that appropriate documentation regarding each back up is maintained. A tape rotation scheme is to be put into operation ensuring tapes are available for all systems. Back up tapes are to be stored on a weekly rota off site at in a fire proof safe in the NRU building.

Informatics Services will take a full back up of all systems.

Back ups are to be tested monthly and a log kept detailing the success/failure of these tests. Failures are to be reported to the appropriate system administrator.

4.2 System and security logs

System administrators (IT Systems Manager / IT Support Manager and Senior Engineer) are to check all logs daily 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.

4.3 Fault Logging

A log of server and network faults is to be kept which records the nature, the duration and the fix applied to correct the fault. The log must show if any outside engineering was required, and if so, by whom.

5. Reporting System Failure Procedures

All hardware or software failures should be reported immediately to the IM&T Help Desk during normal business working hours, and out of hours failures should be reported via pager/telephone to a member of the informatics services on call teem.

All faults must be recorded and stored.

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.