NHSnet : PORTABLE COMPUTER SECURITY POLICY

9.2 Introduction

This document comprises the IT Security policy for Portable Computer systems as described below. For the sake of this document Portable Computers are defined as Laptop and Notebook computers. The security of Digital devices such as PDAs, Palmtops, Advanced Mobile Phones…etc is NOT covered by this document. The policy is issued by the Chief Executive/Senior Partner in accordance with References 1, 2 and 3. All personnel using the Portable Computer system are to comply with this IT Security Policy. Which is based upon elements of BS7799-2:2002. Unauthorised modification and/or amendment of this document is forbidden.
9.2.1 PORTABLE COMPUTER DETAILS/DESCRIPTION:

1. Make:__________________________________________________________

2. Model:________________________________________________________

3. Serial Number:________________________________________________

4. Additional Hardware (HDD etc.):__________________________________

5. Additional Serial Numbers:_______________________________________

9.2.2 HARDWARE CONTROL

The responsibility of ultimate control for issue and security of portable hardware lies with the Chief Executive/Senior Partner. The person nominated to oversee this on their behalf is:

1. Job Title:_______________________________________________________

2. Name:________________________________________________________

3. Telephone Number:____________________________________________

9.2.3 PERSONNEL SECURITY

Only authorised staff are allowed access and use of the Portable Computer System. The NHSnet Connection is not provided for personal and recreational use. Persons accessing data and using it for medical purposes should afford all material stored and processed on these systems adequate protection.

9.2.4 PHYSICAL /HARDWARE SECURITY

The following guidelines should always be adhered to by the user of the Portable Computer:
Treat the Portable Computer as if it is your own property

The Portable Computer must be placed in a securely locked away when not in use. If storage facilities are not available for the Portable Computer then, where possible, the Hard Drive should be removed and stored securely.

Portable Computer security is your responsibility at all times.

If you have and use a Portable Computer security cable, keep one key with you and the other in a secure separate location.

Do not leave the Portable Computer unattended in a public place e.g. car park

Do not leave your Strong Authentication token in the same location as the Portable Computer.

Do not keep password details in the same location as the Portable Computer.

Avoid leaving the Portable Computer within sight of ground floor windows or within easy access of external doors.

9.2.5 STRONG AUTHENTICATION CARD SECURITY

Access to NHSnet is must always be strongly authenticated. That is, a strong authentication hardware token is used to authenticate the user before access is granted. The use of biometric authentication (e.g. fingerprint recognition) providing it meets NHSnet standards is also permitted.

The Strong Authentication Device must be afforded a high degree of protection. Security and confidentiality of patient information could be breached if a card is lost or stolen. The card provides the owner with virtually unlimited access to NHSnet and ultimately any clinical system connected to the network if access rights and privileges are provided/breached. If a card is lost or stolen it is to be reported immediately to the organisations IT Security Officer who will in turn inform the Network Security Manager at the NHS Information Authority.

9.2.6 SOFTWARE SECURITY

Users of Portable Systems are not authorised to load any software onto the Portable Computer system without express permission of the Hardware/Software Control Officer.

Software downloaded from the Internet must not be loaded onto systems containing patient sensitive information.

Software obtained illegally will not be loaded onto Portable Computer Systems.

9.2.7 VIRUS CONTROL

The Portable Computer System must have an Anti-Virus software package installed. Users are not to alter the configuration of this package unless express permission has been obtained from the organisations IT Security Officer. The anti-virus system’s database of virus definitions must be updated on a regular basis, each day if possible.
This package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

If a virus is discovered the following actions must be carried out:

- Turn the Computer off.
- Place a label over the switch and floppy drive stating that the machine has a virus infection and should not be used.
- Isolate any Floppy disks that have been used on that machine.
- Inform the Organisation/Practice IT Security Officer.

The Organisation/Practice IT Security Officer in conjunction with the IT department will have the software and technology available to eradicate any infections.

All virus infections are to be reported by the IT Security.

All serious virus infections which have not been automatically eradicated by the system’s anti virus system must immediately be reported to the NHS Information Authority.

### 9.2.8 PASSWORD SECURITY

Password Security is the responsibility of the individual, passwords should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.

Passwords must not be displayed on screens as they are entered.

When allocated a new/temporary password for start-up use by the systems manager/ administrator the user must immediately change it.

Passwords must consist of a minimum of 6 characters.

Passwords must be changed on change of staff or staff resignation.

Passwords must not be shared amongst users.

Passwords must not be written down.

Passwords should not relate to the system or the user, although passwords must be easy to remember.

Password must be changed regularly, at intervals not exceeding 90 days.

Standard operating system password protection is very limited. The use of other third party software applications to protect both the system and the data contained on it should be considered.
Where sensitive data is to be kept on hard disks the use of an encryption software or hardware package should be considered to provide protection to the data if the machine is lost or stolen.

9.2.9 INTERNET/E-MAIL

The Personal Computer has been provided by the organisation for use off site. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network. It is a source of much valuable information not least on the area of Healthcare, however it is also an unrestricted source of much illegal and illicit material. Additionally it has a large recreational attraction.

Policy for Internet and e-mail use:

Internet and e-mail services will only be used for business purposes directly related to the users area of work.

- No illicit or illegal material will be viewed/downloaded or obtained via the Internet or E-mail.
- Any material downloaded must be automatically virus checked immediately by the Portable Computer’s anti-virus software.
- The user will make their system available at any time for audit either by the local IT Department and/or representatives of the NHS Information Authority.
- Breaches of security abuse of service or non-compliance with the NHSnet Code of Connection may result in the withdrawal of all NHSnet services including E-mail.

Disciplinary Action

Inappropriate use of NHSnet will result in disciplinary action and may ultimately lead to dismissal. It may also be necessary to proceed with criminal charges depending on the nature of the incident.

9.2.10 MAINTENANCE

Maintenance is to be controlled by the IT Security Officer in conjunction with the IT department or nominated person responsible for IT maintenance.

All equipment that requires repair or maintenance must have patient sensitive/confidential information removed from it.

It is not sufficient just to delete files using the computer operating system. The data must be removed correctly using a third party software application that guarantees approved deletion of files.

If the hard disk has failed and the maintenance engineer is required to replace it with a new device then the old hard disk must be physically destroyed. If the hardware is returned to the supplier for repair a note of all serial numbers should be taken including the hard disk. If the hard disk is irreparable organisation must insist that the old hard disk be returned for destruction.
9.2.11 BACKUP

Backup of the system software and configuration must be made on a regular basis.

Regular backups of all critical and/or sensitive data should be made to a separate system where possible to help prevent the loss of critical information. The restoration of backed up data must be tested on a regular basis.

9.2.12 LOSSES AND CONFIDENTIALITY/SECURITY BREACHES

Incidents that constitute a Loss of Hardware or Data, which could potentially lead to a breach of patient confidentiality, are to be reported directly to the organisation IT Security Officer. The Organisation IT Security Officer will instigate investigation procedures to try and establish the nature and potential threat of the incident. All such losses will be reported to the NHS Information Authority.

Incidents could involve:

- Loss of Hardware.
- Loss of Software/Data.
- Virus attack
- Unauthorised access.
- Misuse of System/Privileges.

9.2.13 ACCOUNTING AND AUDIT

The software and information held on Portable Computer Systems is subject to the same audit procedures as the Organisation/Practice Computer Systems. This also covers information and data stored on removable media e.g. floppy disks.

9.2.14 LEGISLATION

Users of portable systems must comply with current legislation regarding the use and retention of Patient information and use of computer systems. These include, but are not limited to:

An explanation of the above can be found in both refs. 1 and 2.
9.2.15 USERS ACCEPTANCE

I have read and understood the Code of Connection document and IT Security Policy detailed above and agree to abide by the requirements laid down in them.

Users signature:____________________ Date:____________________

Approved/Authorised by Name (in Caps):____________________

Signature:____________________ Date:____________________
9.2.16 REFERENCES:

<table>
<thead>
<tr>
<th>No</th>
<th>Title</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NHSnet Networking Security Policy 2002</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Ensuring Security &amp; Confidentiality I NHS Organisations</td>
<td>1</td>
</tr>
</tbody>
</table>

9.2.17 DOCUMENT CONTROL DATA:

<table>
<thead>
<tr>
<th>Security Policy for Portable Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue and Date</td>
</tr>
<tr>
<td>Identity (electronic filename)</td>
</tr>
<tr>
<td>Location of Electronic Copy</td>
</tr>
<tr>
<td>Owner</td>
</tr>
<tr>
<td>Change Authority</td>
</tr>
<tr>
<td>Distribution (electronic)</td>
</tr>
<tr>
<td>Distribution (Paper)</td>
</tr>
</tbody>
</table>
9.2.18 REGISTER OF AMENDMENTS:

This table is to be used to record any amendments made to the Portable Computer Security Policy.

The Policy will be kept up to date and Policy requirements will be constantly implemented and enforced. The responsibility for enforcing this policy lies with the Chief Executive/Senior partner and Nominated Security Officer within the organisation.

Whenever an event occurs which may affect the Policy statements hereafter the Document Control officer must be informed immediately.

On receipt of an amendment instruction responsible security officers must ensure that the amendment is completed as required and that the amendment record is completed.

<table>
<thead>
<tr>
<th>Amendment</th>
<th>Date of Issue</th>
<th>Amended by</th>
<th>Amendment Action Checked (holder)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Published by: Cliff Conrad  
Network Security Manager  
NHSIA - Access to Information

Published: 25 September 2002