Appendix 4 of NHS Lothian eHealth and IM&T Security Policy

Computer devices Controls

1 General

a) The desktop computer is the primary method of accessing electronic information across NHS Lothian. To meet the needs security and confidentiality a number of restrictions are placed upon staff and in the manner with which they access information using PCs. Although there are at present differences between sites in the controls on desktop computers the intention is to produce a standard desktop across NHS Lothian. This policy refers to those standards.

b) Unless exceptional circumstances exist NHS Lothian does not permit the use of shareware or freeware software packages on the infrastructure as it is often difficult to assess the risk that these packages may have on the infrastructure. If a department wish to test a package prior to purchase then approval to do so must be sought from the IT Security team.

2 Clinical Work Stations

a) There are locations where the standard PC would hinder clinicians in their access to clinical applications and where the standard settings are not applicable. Those PCs are referred to as “Clinical Workstations” they are used in areas where at any time several clinical users might require almost simultaneous access to clinical applications. There are restrictions placed upon those PCs.

b) Clinical Workstations have the following characteristics:

c) The logon is hidden and is not to be revealed to non eHealth IT support staff

d) Although access is permitted to the Intranet, access to the Internet is not allowed with exceptions available by agreement (e.g. Toxbase, PECOS..)

e) Individual email accounts are not available

f) All clinical applications available through the clinical workstation will have individual user IDs and passwords.

g) The screen saver will not be password protected.

h) Where departments wish the workstations to be able to access departmental shared drives, those departments shall be responsible for all documentation available on those drives and for any inappropriate comments in or changes made to those documents. Confidential or personal information should not be store in this method.
3 Standard computer device configuration

a) Each member of staff in NHS Lothian shall have their individual network account identity and password. That user ID and password may be used on any normal NHS Lothian computer device. Each user is responsible for their ID and password which they should not share with any other member of staff and should not divulge that to anyone. If their password is compromised for any reason then the staff member should change their password immediately. Guidance on password setting and reminders are given in the Guidance section of this policy.

b) The network ID will allow access to Email, MS Office products, Internet and Intranet. Clinical applications will be available through the desk top but may require an additional ID and password to access those applications.

4 Storage Drives

a) In order to ensure that data is not lost through failures of local drives and to provide staff with access to their information wherever they log on, access to the local computer device hard drive, “C” drive is not available. Each user will be given access to a personal server drive “H” where they shall store any information. That drive will be backed up each night as part of the local support tasks.

b) The use of this drive can preclude the user’s ability to download certain file types from the internet and if this problem is encountered the assistance of the Support Desk should be requested.

c) Users should not use this drive to hold personal, videos, games, music (MP3) or other non work related files.

5 Remote Management

a) Each computer device is capable of being managed remotely and this facility may be used when a user places a Service Desk call because of a problem. The use of a remote management tool will be discussed with the user by the support desk and a warning that it is in use will be shown on screen. The remote management toll is configured in such a manner that it is not possible to use without informing a user. This is to mitigate potential breach of the Regulation of Investigatory Powers Scotland 2000 (RIPS) which could lead to prosecution of any member of staff who took that action.

6 Antivirus

a) All computer devices in NHS Lothian are protected by an antivirus product. This product runs in the background and is automatically updated several times each day. Users are not to attempt to stop any updates especially during initial start up of the PC. Computer devices without this product may not be connected to the network.
7 Use of Storage Devices

In order to protect confidentiality the ability to “Write” to external devices has been restricted on PC’s by default. This includes the permissions to write data to USB Pensticks, Digital Camera’s, memory cards and other mstorage devices. Where a user requires the ability to write data to a USB Device, encrypted memory sticks are available to staff. An application should be made using forms available on the intranet. If it is believed that Identifiable person data needs to be stored on a Penstick or other USB device or non network drive, this must be encrypted and/or application is to be made to the Caldicott Guardian for permission to do so. This includes video and audio recordings.

8 Software

a) The computer devices throughout NHS Lothian are optimised for the use of clinical applications. Where it is necessary to load additional software onto a PC consideration must be given not only to the single user but also to the needs of the applications used through out the organisation which may be effected by conflicting requirements. It is therefore necessary to prevent users having the ability to load software onto any PC or network server. Where it is believed that software is required to be loaded onto the network then the local Support desk should be contacted for advice and especially prior to purchase of any packages which may impact on clinical services.

b) No software which is not owned and licensed to NHS Lothian is to be loaded onto a desktop or server including games, music or video applications without the permission of the IT Security.

9 Port Control

a) All computer devices have software installed that restricts the use of devices that are plugged into any interface on the PC. This can include but is not limited to:
   - USB Pensticks & Hard Drives
   - Digital cameras
   - USB Printers
   - Dictation Equipment
   - Modems & Wireless Interface Cards
   - Tablet

No non NHS Lothian owned device should be connected to the network via a PC without authorisation by IT Security.

Where appropriate all users by default have the ability to read & write to these devices but some services are restricted. If access to a device is required then a request should be made to the IT Security Department.
Read Only restrictions are in place with all removable media unless the device is an NHS Lothian provided encrypted device.