Identity controls including Access to Applications and Network

1. NHS Employees

a. It is policy of the Scottish Government that all NHS staff have access to email, internet, intranet and applications, both clinical and administrative, to facilitate them in carrying out their role and responsibilities in the support and management of patient services and to facilitate their training.

b. To enable this it is necessary to provide each user with access to the network and to the various applications. “Single sign on” for specified systems is available, in addition to Virtual Desktop access cards.

c. Each employee, during their induction process, will be provided a form by HR, which when completed and appropriately authorised an approved signatory, will allow that person access to the network, email, internet and major applications as required. As part of that process the new user will sign that they have read and understood those parts of this policy, which are attached to the form, mainly those relating to appropriate and inappropriate behaviour, confidentiality and use of email and the internet.

d. Those IDs will then be activated after the employee has been trained in the appropriate systems and applications. It is not within the remit of a manager to attempt to deny access to email or the internet to a member of staff, only to ensure that correct applications are selected and that the level of access to the applications i.e. the security group for the application is confirmed. Each site will continue, for the foreseeable future, to have minor differences as to where this training and allocation of ID is presented to the user.

e. As part of the creation of the user ID each user will be allocated by eHealth a “Home” Directory or drive. That drive will be held on a server and backed up as required by Appendix 8. The user will not have access to the local “C” drive. Where departmental or shared drives are required the user will be instructed by the departmental “owner” how information on those drives is to be recorded.
2. Non NHS, Non University employees including Bank and Agency

a. Where a non NHS employee, contractor, or volunteer requires access to the network a separate application will be made by their NHS sponsor for them to be allowed access to specific services or devices. These applications should be discussed with IM&T security prior to any agreement being reached or contract signed as what might seem to the contractor as reasonable may breach other internal or external connectivity agreements.

b. A standard NHS Lothian Network access form must be completed to request access. The NHS Lothian sponsor is responsible for ensuring the applicant has read and understood obligations to NHS Lothian eHealth security policy and under legislation

c. A register of non-NHS Lothian users should be held and regularly reviewed by eHealth.

3. University and Research staff

a. Before an application will be processed for a member of the University of Edinburgh staff or for a researcher who does not already hold an NHS contract of employment, a honorary NHS contract or a letter of Research Access must be granted by the joint (University/ NHS) Research Office.

b. There are specific methods for the interconnection between the University of Edinburgh and the NHS, how it is to be achieved and its management; these are outlined at Appendix 5.

4. Password Controls

a. The network and all applications are to be password protected. Each user is responsible for maintaining the security of their passwords for their network and application ID. Staff are not to write down their password and leave them where they may be overlooked or found by unauthorised persons. Passwords are not to be shared with others. During any investigation into unauthorised or inappropriate access to systems or material, where a person claims that they shared the password with others and are therefore not responsible for any misdemeanour will not be accepted in defence but the person declaring such will be automatically in breach of NHS Lothian policies and therefore subject to disciplinary action.

b. To facilitate the maintenance by users of passwords all systems will be set where feasible to force users to change their
password every 42 days. Staff are provided information in how to select and manage passwords at:
c. “Guidance Note 1 Setting Passwords” to this policy. Where the ability exists in applications to force complex passwords e.g. over 6 letters and containing alpha-numerics, it shall be set to force that action.

5. Leavers

a. Each month Human Resources will supply the System Administration Team with a list of leavers from NHS Lothian. The users IDs will be made inactive immediately but the “Home” drives will be maintained for 3 months unless request for additional time is agreed with eHealth. During this period if a department wishes to access any business information stored on the drive an application should be made to by the service manager to the eHealth security officer to arrange the access or movement of files.

b. If a person has been or is about to be dismissed or suspended by NHS Lothian, Human Resources or the line manager are to inform eHealth immediately so that the ID may be blocked to limit any wilful damage that might be done subsequent to that event.

6. Access to Records

a. Throughout NHS Lothian there are a number of areas where health, staff and corporate records may be held on a variety of media including paper and electronic. Access to this information, particularly that information deemed as sensitive under the Data Protection Legislation, mainly but not exclusively, Health and Human Resources must be controlled. All records must be retained in accordance with the NHS Lothian Records Management Policies, where sensitive records are held in an area to which access is to be controlled.

b. Access to records must be in compliance with Data Protection Legislation. A written request must be made to the Legal Services Manager or Data Protection Officer. Access to your own or records of those whom you do not have a NHS Lothian role in care or administration is not permitted. Access is monitored for this purpose.

7. Server Rooms

a. Server rooms are by their nature one of the most vulnerable areas of the IM&T infrastructure. To prevent loss or damage of
the equipment held in these areas strict access controls are to be applied. Server rooms are to be locked at all times and a record is to be maintained of those accessing them. This record may be electronic where an electronic swipe or other access system is in place. The access records are to be checked at least monthly and access lists reviewed at that time. Where an electronic process is not available a record is to be kept of all entering and the purpose of that entry.

- Records of those who have been given the door access pin code will be maintained by the Server Team Manager, who will arrange to change pin codes every 3-month and inform IT security Manager of the active dates of new pin codes. Pin codes also will be changed if a staff member leaves or changes job role and no longer requires access.
- Electronic door access lists should be reviewed by Server Team Manager every 3 months and inform IT security Manager of completion. If a staff member leaves or changes job role, the access right of this staff member should be removed.
- Records will be maintained of keys issued to staff members with detailing who has keys and when they were issued. Keys must be returned when a staff member leaves or changes job role and no longer needs access.
- If keys are shared, they will be stored securely and there will be a record in place to log when and by whom the key has been ‘used’.
- External contractors are not to be allowed unrestricted access to server rooms and are to be accompanied whilst working in those rooms.

b. Server rooms are to have wherever possible air conditioning of sufficient capability to maintain the room within the ideal temperature range for the equipment operating there.

c. All server rooms should have uninterruptable power supplies sufficient to maintain the servers where there is a loss of mains power. Allowing the servers to operate normally or to allow a controlled shutdown of the servers in the event of a sustained period without power.

d. Server rooms should have fire suppressant equipment installed which is capable of operating in a manual or automatic mode.

e. Where it is necessary to base servers outside dedicated server rooms, e.g. small Medical Practices, those servers should be placed in a room which can be secured (risk assessment
available), has sufficient ventilation, is not close to heat sources and is relatively dust free. The server should also be fitted with a UPS which will allow automatic shutdown of the server if mains power is lost.