Business Continuity and Disaster Recovery Plans

1. The IM&T systems throughout NHS Lothian are critical to providing services directly for patients. Without these systems patient care cannot be delivered at an appropriate level. It is essential that processes and procedures are in place and tested which will allow NHS Lothian to provide patient care with minimum disruption at any time or for any reason. As part of the National Critical Infrastructure the NHS has a responsibility to protect that infrastructure and a legal requirement under Civil Contingency Act 2004 to have a continuity policy in place to cope with major incident, civil disaster including a pandemic.

2. Previously NHS Lothian’s IT infrastructure was coterminous with its provision of service, its outer perimeter however no longer ends at the boundaries of NHS Lothian. With a number of international companies supplying services to NHS Lothian through internet connections and an increasing number of staff remotely accessing clinical systems and other services from home and elsewhere it is now world wide. It is therefore necessary to impose restrictions on its use to prevent abuse.

3. The critical areas may be broken into several categories:
   i. Network
   ii. WAN & LAN
   iii. Servers
   iv. Clinical Systems
   v. Trak/PAS/PIMS
   vi. Investigations and Monitoring
   vii. Ilab/PACS/RIS
   viii. Clinical Reporting Systems
   ix. Vision/SCI results/Gateway/UCS
   x. Non Clinical systems
   xi. Email
   xii. Finance and procurement
   xiii. PCSMR
4. Network

   a. The network may be exposed to various types of incident:
      i. Physical Disruption through accidental or deliberate damage
      ii. Denial of Service through “malware” or email attack.

5. Disruption through Damage

Whilst it is possible that elements of the Wide Area Network (WAN) could be subject to an terrorist attack occurring at, or close to a building where one of its numerous switches are based, disruption of the service is most likely to be achieved by a person accidentally cutting through a cable during road maintenance. There is by the nature of the WAN, sufficient redundancy on routing between the main sites to avoid total loss of services to all sites. Should such an event occur the most likely occurrence would be an apparent slowdown of access to the various systems.

Should this occur, a warning will be sent to all users to reduce email traffic to a minimum and restrictions would be placed on access to the internet.

6. The WAN is maintained by Capita as part of the SWAN (Scottish Wide Area Network) national network procurement. It is possible that some health centre or community hospital which have only a single connection from the WAN might be isolated and lose connectivity whilst repairs are carried out.

7. All network communication and node rooms containing network switches and other devices are to be locked and access to those rooms restricted. An access list is to be maintained. Contractors or other unauthorised staff are to be accompanied whilst in these areas.

8. Denial of Service

9. A denial of service attack can be initiated through a number of events; the introduction of a Virus, Trojan or Worm into the network from sources including, external email, CDs, Pensticks and other USB storage devices. It can be triggered by a member of staff creating a chain email and it being forwarded to and from other staff. This effect simulating heavy traffic can also be produced by some “spyware” being introduced to a computer device whilst the user is on the internet.

10. To reduce and mitigate the effect of such attacks NHS Lothian has a number of defences in place including; Intrusion Detection Systems, antivirus applications, restricting the number of staff able to send
“everyone” emails, restricting access to the network to NHS devices and NHS approved organisations, only allowing staff access to USB devices after a clear business or clinical need has been established.

11. NHS Lothian also filters incoming and outgoing mail for known virus definitions and blocks certain types of files which are known to present an increased threat to its services. This functionality is described at Appendix 2.

12. All NHS Servers and PCs attached to the network are to have active NHS Lothian provided AV applications running to prevent virus or other attack

13. Clinical Systems

14. All the major clinical systems are server based and the servers are to be situated within Server rooms.

15. The server rooms are to be locked and access controlled. An access list is to be maintained and a record is to be kept of all staff entering the server room. Where entry is via a swipe card the entry log must show who entered the room and when they did so. Contractors and others not on the access list are not to be allowed un-supervised access to the server rooms.

16. All servers should be connected to either an individual or room served, Uninterruptible Power Supply (UPS). The UPS is to be capable of allowing a controlled or managed shutdown of the server(s) in the event of a loss of power.

17. The UPS when it is activated should be capable of sending a warning message to an IT Support team.

18. Server rooms are to have air-conditioning fitted wherever necessary to allow the servers to operate within their optimum temperature range regardless of the outside temperature

19. Servers

20. All servers are to be backed up in an approved cycle. This cycle should provide the ability to restore both the operating system and the data in the event of a failure. The back up media is not to be left with the server but removed and placed in a different location.

21. Where systems are deemed to be critical, a secondary or back up server is to be provided which will automatically take over the role of
the primary in the event of its failure. This secondary server should ideally be in a different location to the primary.

22. Where a secondary server is not available a risk assessment is to be carried out on the effect of the loss of the server and those results held within the NHS Lothian or Operating Division Risk Register.

23. The NHS Lothian Server team is to carry out a full restore of all critical servers annually.

24. Where a contract exists for the provision of server hardware in an emergency, this is to be rehearsed, if necessary in the contractor’s premises and the operating system back up and the data restored within the agreed time limits. Each restore is to be logged and a report produced highlighting any issues raised and the remedial actions required.

25. A GP system server back up from each NHS Lothian GP system site is to be restored twice each year into the eHealth test environment and any faults reported and resolved.

26. Each contract for a managed service of hardware for major clinical systems is to include an annual failover of that system.