NHS ORKNEY

BACK-UP PROCEDURE

Date	Version	Comments
March 2010	V2.1	
December 2011	V2.2	Revised following IT Internal Audit Report 01.10/11

1. Statement

   It is essential that adequate, verified back-ups of all the Board's computer systems are taken on a regular basis to ensure the continued operation of the Board's systems.

   Back-ups of the following systems shall be taken:

Windows Servers	:	Server Farm
IBM 610 6EI	:	Laboratory System
E-Manager	:	Telephone System
Call Logger	:	Telephone System

2. Responsibilities

   It is the responsibility of the Computer Officer to ensure that verified back-ups are taken and that this procedure is adhered to.

   In the absence of the Computer Officer the Technical Support Assistant shall be responsible for following the back-up procedure.

3. Back-up Storage

   Recent backup tapes must be stored in the fireproof safe located at the Selbro Store, Hatston.

   Older backup tapes may be stored in the Central Stores fireproof safe.

4. Tape Rotation

   Only tapes from reputable manufacturers shall be used.

   The back-up tapes shall be rotated as follows:

Monday – Thurs	:	the tapes are re-used each week
Friday	:	one tape for each Friday in the month, except the last.
Month	:	one tape for the last weekday in each month, tape to be retained.

5. Tape Cleaning

   Each tape unit must be cleaned using appropriate cleaning materials.

6. Back-up Procedure

   Backups shall be taken out-with office hours, where possible.

7. Backup Media

   Backups will be taken to disk and then to tape.

8. Backup Policy

   Monday- Thursday backups will be incremental; Friday backups will be full backups and clinical systems will be given priority. Because full backups taken on a Friday will last into a weekend only clinical systems will be backed up incrementally over the weekend.

9. Backup Licences

   Agent licences shall be used to backup file servers, e.g. File Agents for Windows File System, SQL Agent for SQL databases and Exchange Agent for MS Exchange.

10. Disaster Recovery Testing

A DR test will be carried out each quarter. A DR test scenario will be agreed beforehand, the DR test will be fully documented and any issues with the DR test will be investigated and resolved before the next DR test.

11. Fault reporting

Any faults encountered (i.e. hardware, software and unsuccessful back-up/verify) should be resolved before the next backup cycle.

Faults should be reported to the IT Manager.