

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

Name	Job Title	Signature	Date
Authored by:- <Name>	Technical Support Officer		
Approved by:- <Name>	Information Security Officer		
Authorised by:- <Name>	Director of Finance & IT		

2. Change History

Version	Date	Reason
Draft 1.0		First draft for comments
Draft 1.1		Amendments to Appendix 3
Version 1.0		First Version
Version 1.1		Amendments to tape back up record sheet

3. Contents

1. Approval and Authorisation.....	1-1
2. Change History	1-1
3. Contents	1-2
5. Introduction	1-3
6. Data Backup Statement.....	1-3
7. Information Back-up Process	1-3
7.1 Overview	1-3
7.2 Storage.....	1-4
7.3 Safety.....	1-4
7.4 Tape Change Procedure.....	1-4
7.5 Back-up Procedure.....	1-5
7.6 Back-up checking and verification.....	1-5
Appendix 1 - Machines that are backed up each week-day evening.....	2-1
Appendix 2 - Ground rules for working in the computer room.....	3-1
Appendix 3 - Computer room keys and extinguishant system.....	4-1
Appendix 4 - Loading and unloading tapes for the different types of drives.....	5-1
Appendix 5 - Rota of back-up tapes.....	6-1
Appendix 6: Tape Change Log (TCL).....	7-1
Appendix 7: ENERGY backup.....	8-1
Appendix 8A: To run the daily checks on the (Example) DEC Alpha.....	9-1
Appendix 8B: Daily Tasks Check List & Results – (Example) DEC Alpha.....	10-1
Appendix 9: Back-up procedure.....	11-1
Appendix 10: Synchronise procedure.....	12-1

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

5. Introduction

To allow data essential to the business of the Trust to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems.

In order to achieve this there must be set procedures to cover:

- a) the copying of data to a medium which can then be stored in a secure place (back-up).
- b) the retrieval of data from copy made on the medium in a) above (restore).
- c) the secure storage of media containing the data copies made in a) above.
- d) the recording of details about the media and what data it stores to facilitate the easy and correct identification of a particular item of storage media when it is necessary to retrieve data from it, as in b) above.
- e) testing the quality of the back-ups made in a) above both by log checking, verification techniques and by test retrieval of data from an item of storage media.

6. Data Backup Statement

It is the policy of the NHS TRUST that all central systems will have daily backup regimes formalised in the appropriate job run manual. Such backups will have a minimum of five days cycle before media is overwritten.

All networked PCs will use the designated drives on the server. Under no circumstances should data be stored on the local drives of PCs which are connected to the network. Floppy disks etc. must never be used to store data, but only for transferring data."

7. Information Back-up Process

7.1 Overview

These procedures only cover the centralised computer systems and servers controlled by, and operated for the Trust's behalf, by the IT Operations department. The machines that fall with these criteria (ie needing to be backed-up by the IT Operations department) listed in Appendix 1.

It should be noted that these servers are the ONLY computers that are backed up by the IT Operations department. Generally, all data and information on computers should be saved only on the Cxxx system - whose data is backed-up using the procedures outlined in this document. Data stored anywhere else (eg on a PC's hard disk) will NOT be backed-up by these procedures. IN SUCH A CASE ANY DATA NOT STORED ON THE CXXX SERVERS (or other servers backed up in these procedures) WILL BE LOST IF THE MEDIUM IT IS STORED ON IS LOST OR DAMAGED OR OTHERWISE MADE UNREADABLE.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

(Homeworkers who dial-in to Cxxxx can use the "Synchronise" procedure to copy files on their Trust-owned home computers to Cxxxx. These files, once copied to Cxxxx, will be backed up as part of the overnight back-ups described in this document. Instructions on using the "Synchronise" facility can be found in Appendix 10 of this document.)

There are five sections to ensure that the Trust's information and data systems on computer are backed-up safely and correctly.

7.2 Storage

The tapes are kept in a locked fire safe in the underground car park of <Site 1>. One set is kept in an off-site archive for security purposes.

The tapes must be stored upright (ie standing on one of the "narrow" sides) and not lying down.

The computer room is in the basement, the last door on the left when leaving the building via the doors to the underground car park.

7.3 Safety

For safety reasons nobody is to enter the computer room on their own, therefore tape changing must always be carried out by 2 members of staff from the IT Operations Department. Please see Appendix 2 - Ground rules for working in the new computer room.

All rules for staff safety are to be observed while working in the computer room.

7.4 Tape Change Procedure

The tapes are changed every normal working day (ie weekdays except Bank Holidays).

1 The keys to the fire-safe & the computer room are kept in the key box by the Helpdesk Administrator's desk in the IT Operations room. These are collected and signed for by one of the people who are changing the tapes.

2 The tapes for the day are collected from the fire-safe (in a box so that the tapes do not run the risk of damage by dropping them).

The fire extinguishant & alarm system must be disabled, using the appropriate keys, on the control box on the wall outside the computer room. The keys for doing this are held by Reception and they must be signed in & out by one of the staff changing the tapes. See Appendix for procedures on operating the control box.

4 The computer room is unlocked (both the metal & inner wooden doors) and the IT Operations personnel can then enter the computer room and change the tapes.

5 The tapes are unloaded. See Appendix 4 on how to unload the tapes for each of the different types of drives.

6 Once unloaded the tapes in the machines (from the previous working day) are, in turn,

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

removed and the current day's tape (see Appendix 5 for rota of tapes to use) for that machine is inserted and loaded. See Appendix 4 for how to load the tapes for the different types of drives.

7 When all the tapes have been changed the computer room is locked and the fire extinguishant and alarm system is reset using the control box – see Appendix 3. The keys to the extinguishant & alarm systems and the outer, steel door must be returned to Reception.

8 On Mondays to Thursdays the previous working day's tapes are placed back in the fire-safe and locked up. On Fridays, the Thursday night back up tapes are sent to off-site storage – see Appendix 5 for this procedure.

9 The keys are returned to the box in the Helpdesk Administrator's desk and signed off by one of the two people who changed the tapes.

10 Details of the tapes used for that day are entered in the tape change log (TCL) – see Appendix 5.

7.5 Back-up Procedure

For the majority of the Trust's systems the backing up procedure occurs automatically and out-of-normal working hours. This is in order that there is minimal disruption to the service offered to users and to ensure the integrity of the data and information being backed-up.

All systems are backed up fully to tape – ie the back-ups are not differential – every file is backed up every night.

Systems on xxxx xxxxx xxxx servers: ie xxx-2, xxx-4, xxxx-1, xxxx-2, xxxx-3, xxx-3, xxxx-2 and xxxx-12

These servers are backed-up automatically using Arcserve software. The process starts around 11.0 pm every week-day night.

xxx-xxxxx

This server's back-up starts around 1.10 am each week-day morning using a job entry in the server's "cron".

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Energy

The back-up for the Energy system is initiated manually by the IT Operations department at a time when the is not too busy doing other operations. This is generally at some time during each working day's afternoon.

The initiation procedure is described in Appendix 7.

7.6 Back-up checking and verification

xxx-2, xxx-4, xxxx-1, xxxx-2, xxxx-3, xxx-3, xxxx-2 and xxxx-12

Daily back-ups are checked by visual checking of the output logs by the Network/Systems Supervisor.

Less frequently, verification that data is being correctly written to the back-up tapes is made when a user's files are restored to the systems.

xxx-xxxxx

A logging system is in place which can be used to look at detailed aspects of the overnight back-up of both the National Database and the Unix system in general. This is used to produce an exception report when various parameters, in the back-up, change. This report is checked by the IT Operations Manager. Appendices HA & HB give details of all checking and verification procedures for the xxx xxxxx when done manually and indicate the types of check done when through the automatic system.

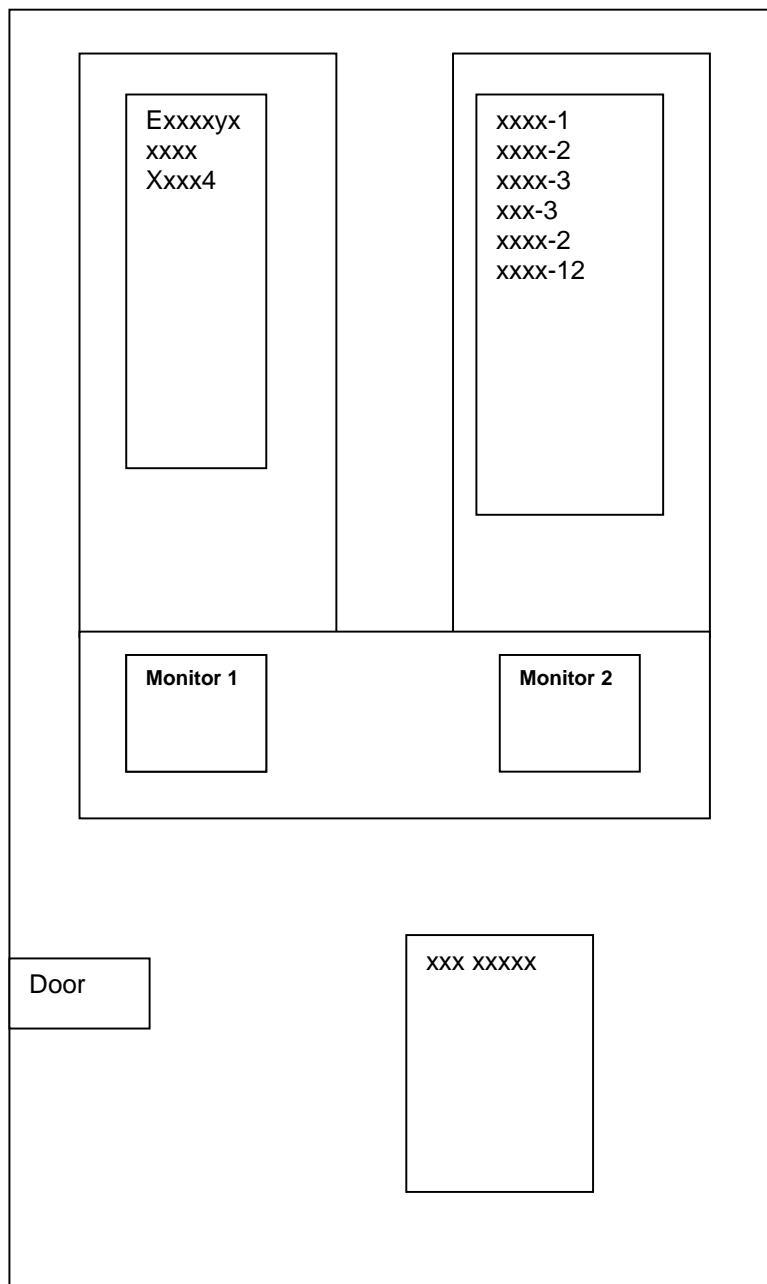
The back-up system for the DEC Alpha is at the Trust's <Site 2> site. From time to time tests are made to ensure that a back-up on the <Site 1> xxxxxxxxx can be re-loaded onto the <Site 2> xxx xxxxx server. See Appendix 9 for information about restores etc. (Note the backup procedure in this document is no longer used, currency of all information within Appendix 9 should be verified before use.)

Energy

Every day a visual check is made to make sure that the previous day's back-up finished OK. (Ie the session running the back-up has return to the "Pick" command prompt.) Once a week a verification check is made to ensure that the back-up has written to the tape correctly. The procedure for running the verify is given in Appendix 7 step 4.

Appendix 1: Machines that are backed up each week-day evening

The machines that currently need backing up to tape are as shown below in the Computer Room diagram (as at 12th September, 2001 there are 10 machines):



Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Appendix 2: Ground rules for working in the computer room

These rules are not violatable by anyone except by the IT Operations Manager [or in his absence] the Desktop Systems Development Manager) who can allow the procedures to be violated. Any violation will be considered a severe disciplinary offence - these rules exist to protect staff working in this area.

1. Only IT Operations or Systems department personnel can enter the room - all others must be approved by the IT Operations Manager or the Desktop Systems Development Manager and escorted by 2 IT Operations staff.
2. No-one is to enter the room alone – only the IT Operations Manager or the Desktop Systems Development Manager.
3. The fire suppression system must be disarmed when staff are in the room.
4. All tasks that can be done from remote consoles must be done from there.
5. Nobody will be forced to use this facility, however objections must be registered, in advance, with the IT Operations Manager.
6. Cover rosters must include this information.
7. There MUST be TWO people capable of entering the computer room on duty between 9am and 5pm.
8. Safety training will be given.
9. Any problems or concerns about the computer room should be reported to the IT Operations Manager or the Desktop Systems Development Manager. Every concern will be investigated.

Appendix 3: Computer Room Keys and Extinguishant system

For information: The following documents give further information on the fire alarm & extinguishant system should the need arise.

The current daily procedure is in [Document 1](#).

Documents 2 & 3 are largely now obsolete and for information only.

Document 1 - Procedure for entering the Computer Room

- 1 Collect Computer Room key & safe key from the Helpdesk & sign them out.
- 2 Collect Outer Store & Fire Extinguishant keys from Reception and sign for them in the Visitor's Book.
- 3 Proceed to the Computer Room outer door.
- 4 Select the "delta" headed key and insert it in the "Mode Select" key hole on the front panel of the Fire Extinguishant System panel (see Figure 1).

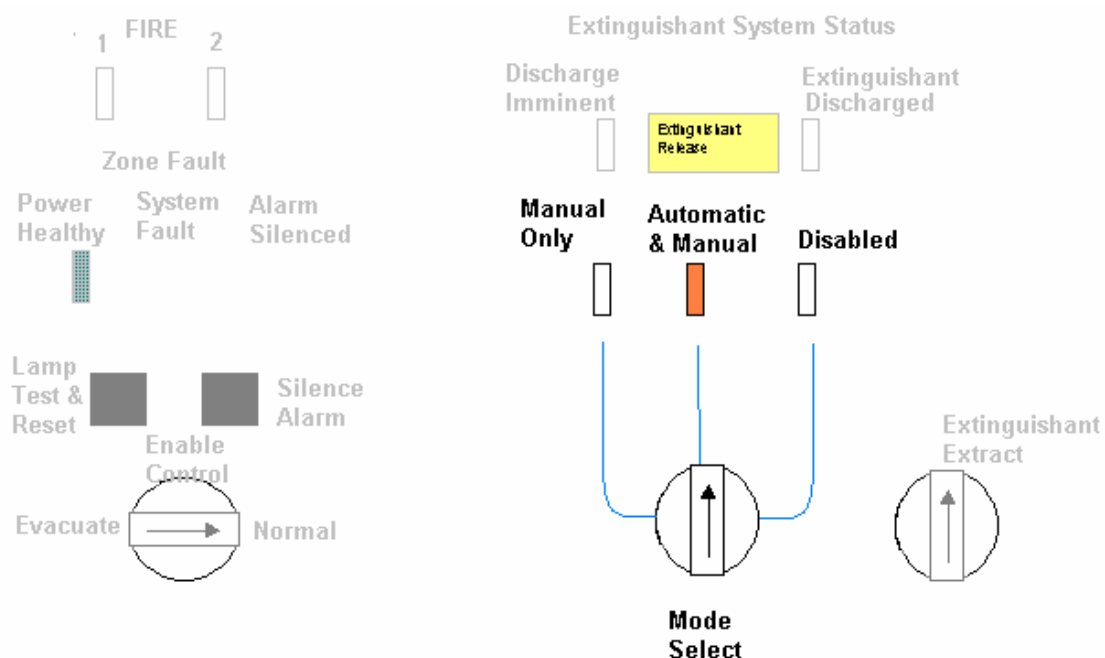


Figure 1.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

5 Turn the key to the left so it points to "Manual Only". A green light comes on. Remove the key.

6 Use the appropriate keys to unlock the steel-faced outer door and the wooden inner door.

7 Change the tapes according to the relevant sections in this document.

8 Leave the computer room and lock the doors.

9 Insert the "delta" headed key in the "Mode Select" key hole on the front panel of the Fire Extinguishant System panel. Turn key to "Automatic & Manual". The orangey-yellow light comes on (see Figure 1).

10 Return the Outer Store & Fire Extinguishant keys to Reception and sign them back-in in the Visitor's Book.

11 Return the Computer Room key & safe key to the Helpdesk & sign them in.

Should an emergency occur while staff are in the Computer Room

One of two safeguards are in place:

1 There is a "panic button" in the corner of the Computer Room adjacent to the DEC Alpha. If an emergency arises while staff are in the Computer Room they should press the "panic button" which will raise the alarm at the <Site 1> Reception desk who will arrange the appropriate response.

2 If staff do not return the Outer Store & Fire Extinguishant keys within a short period of collecting them the staff on Reception will arrange an appropriate response.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Document 2:

This procedure is superseded by Document 1 above; this procedure is included for further information that it may contain.

**TEMPORARY PROCEDURE
RE-SETTING FIRE SUPPRESSION SYSTEM
BASEMENT OPERATIONS ROOM**

The Fire Suppression detection system is currently in a testing stage before hand over.

If the system should activate the siren within the Operations Room will sound and the warning strobe light in Reception will activate.

The fire suppression gas **will not** be released, and the buildings main fire alarm will not be activated.

If the suppression system activates one of the following personnel should be contacted to re-set the system.

xxxxxxxxxx – Facilities Manager – Ext xxxx
 xxxxxxxxxxxx – Assistant Facilities Manager – Ext xxxx
 xxxxxxxxxxxx – I.T. support – xxxx

RE-SETTING

1. Insert key into left hand key switch.
2. Turn key anti-clockwise to ENABLE CONTROL.
3. Press silence alarm.
4. Enter the Facilities Store Room and Operations Room.
5. Check which detector(s) have activated and make a note. (detector will have a small light illuminated).
6. Leave area and secure door
7. Press the button on the panel marked LAMP TEST & RESET
8. Turn key clockwise to NORMAL and remove key.

Note

If the above procedure fails to silence the internal sounder Contact
 xxxxxx PROPERTY MAINTENANCE. – xxxxx-xxxxxx

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Document 3:

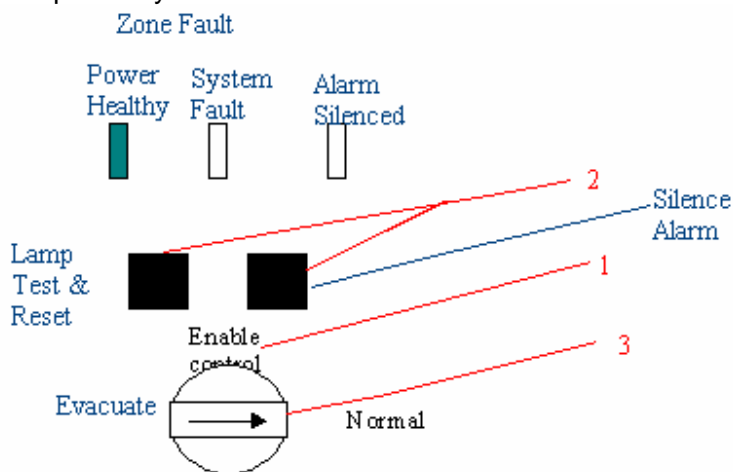
This procedure is superceded by Document 1 above; this procedure is included for further information that it may contain.

If the alarm in the new computer room goes off

THE EXTINGUISHANT SYSTEM & ALARM SYSTEM ARE NOW OPERATIONAL – BOTH SYSTEMS ARE TO BE TURNED OFF AND THE ROOM UNLOCKED BY THE FACILITIES MANAGER (OR DEPUTY) BEFORE THE ROOM IS ENTERED (SEE ABOVE NOTES AND ASSOCIATED PROCEDURE DOCUMENTS).

The only time someone will hear the alarm is if they pass the room. They will then alert Reception who will alert IT to turn off alarm (if facilities management aren't around).

The panel layout is:



- 1 Insert key & turn to "Enable control"
- 2 Press Silence Alarm.
- 3 Enter the Facilities Store Room and Operations Room.
- 4 Check which detector(s) have activated and make a note. (detector will have a small light illuminated).
- 5 Leave area and secure door.
- 6 Press the button on the panel marked LAMP TEST & RESET
- 7 Turn key back to Normal.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Appendix 4: Loading and unloading tapes for the different types of drives

DLT: xxxx xxxxx xxxx machines: ie xxx-2, xxx-4, xxxx-1, xxxx-2, xxxx-3, xxx-3 xxxx-2 AND xxxx-12

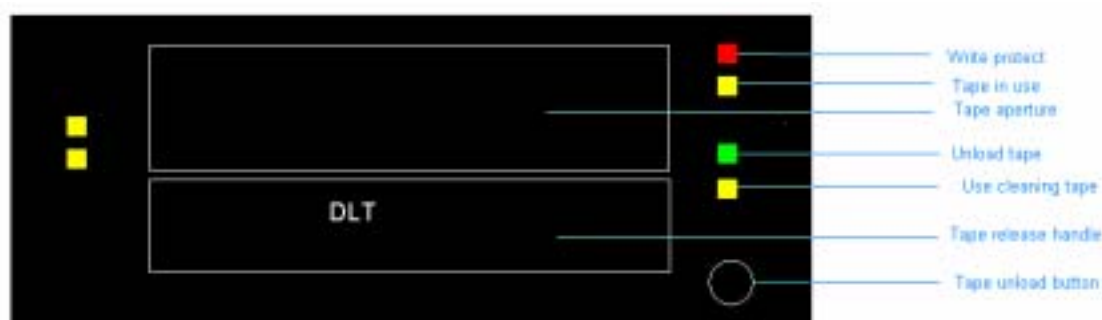


Figure 1.

- 1 Press the "Tape unload button".
- 2 Wait until the green "Unload tape" light appears. ALL OTHER LIGHTS MUST BE OUT BEFORE REMOVING TAPE (step 3 below).
- 3 Lift the tape release handle. The tape will move out slightly of the "Tape aperture".
- 4 Take out the tape, place it in its box.
- 5 Put today's back up tape in the "Tape aperture" and push it "Home".
- 6 Push the "Tape release handle" down to lock the tape in.
- 7 When "Tape in use" and the two yellow lights on the left hand side are lit the tape is loaded correctly ready to start the back-ups.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Other lights

1 The "Write protect" light shows if the tape is write protected (using a slider on the "spine" of the tape). This means that the back-up will not work until the tape is "un-write-protected".

2 "Use cleaning tape" light indicates just that! A cleaning tape should be inserted in the "Tape aperture" (as in steps 5 & 6 above. The tape will go through a "load" process as it runs the tape through the drive. It will then unload itself automatically. When the green "Unload tape" light shows lift the "Tape release handle" and remove the cleaning tape. Hopefully the "Use cleaning tape" light will have gone out and the normal back-up tape can be placed into the "Tape aperture" as in steps 5 & 6 above.

xxx xxxxx DLT

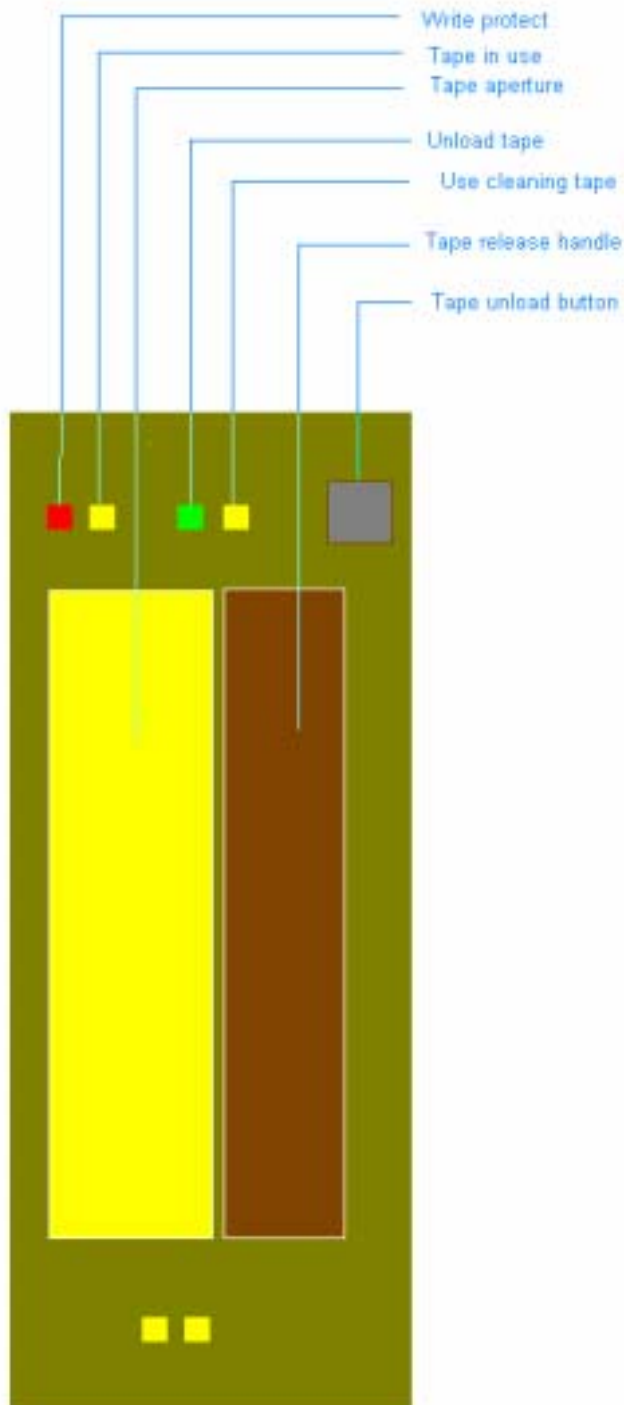


Figure 2.

The DLT drive on the xxx xxxxx (which holds the xxxxxx xxxxxxxx Database and the xxxxx xxxxxx systems) is more or less the same as the xxxx xxxxx xxxxx (above) except it is mounted on its “side” – see Figure 2.

The main operational difference when changing tapes is that the DLT tape is normally rewound when the back-up has been completed. This means that when the tape is being changed the green “Unload tape” light will already be lit. (If this is not the case the IT Operations Manager should be consulted before proceeding.)

The steps to change the tape are:

1 Make sure that the green “Unload tape” light is lit. ALL OTHER LIGHTS MUST BE OUT BEFORE REMOVING TAPE (step 2 below).

2 Lift the tape release handle and move it from right to left (as opening a door). The tape will move out slightly of the “Tape aperture”.

3 Take out the tape, place it in its box.

4 Put today’s back up tape in the “Tape aperture” and push it “Home”.

5 Push the “Tape release handle” to the right (like closing a door) to lock the tape in.

6 When “Tape in use” and the two yellow lights, on the bottom of the drive, are lit the tape is loaded correctly ready to start the back-ups.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

The Energy system

This system uses a DAT tape drive (see Figure 3) which takes a 120m DAT tape.

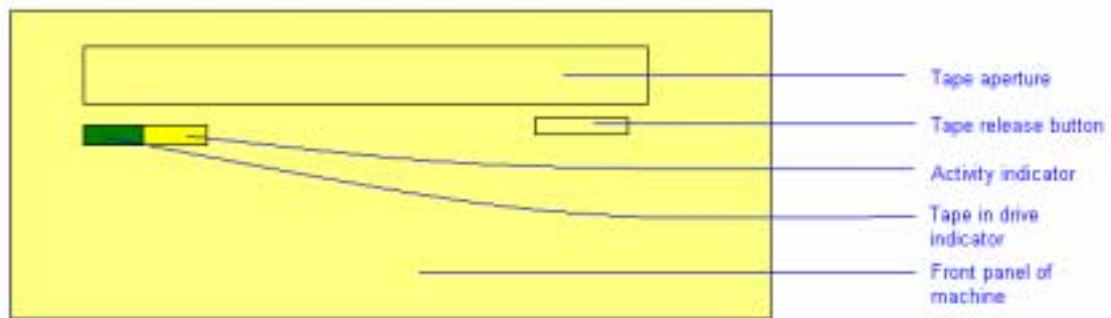


Figure 3.

- 1 The "Tape in drive indicator" should be lit to show a tape is currently loaded.
- 2 Press the "Tape release button" – the "Activity indicator" should light.
- 3 When the tape has rewound it is ejected at the "Tape aperture". Both the
- 4 Remove the tape and place today's tape in the drive. Both the "Activity indicator" and the "Tape in drive indicator" should now be out.
- 5 Gently push the tape in until the load mechanism is felt to engage (rather like a home video tape machine). Both the "Activity indicator" and the "Tape in drive indicator" should now be on.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Appendix 5: Rota of back-up tapes

There are nine sets of tapes used in to back-up the Trust's various production systems at <Site 1>, <Site 1>.

Currently (24th September, 2001) there are 10 tapes allocated for each day (Monday to Wednesday and Friday). These are rotated on a weekly basis – each set being overwritten once a week on its allotted day.

There are four full sets of tapes for Thursdays – each set being rotated on a four-weekly cycle so that every fourth week it is overwritten. Thus a set of Thursday tapes is overwritten every four weeks.

A tenth set of tapes is designated “Special” and is used to do back-ups in special circumstances – for instance, in periods where there are multiple bank holidays and no staff are changing the tapes. (All DLT-tape using machines except the xxxxxx leave their tapes loaded allowing the next back-ups to overwrite the ones already on them. The xxx xxxxx unloads the tape so overwriting the tape on consecutive nights does not take place.) The xxxxxx tape is not knowingly overwritten as its back-up process is manually initiated when the tape is changed. However, for completeness, both the xxxxxx system and the xxxxxxxx are included in the “Special” set of tapes.

The tables below show the tapes changed for each day:

Day/machine	xxxxxx	xxx-2	xxx-4	xxxx-1	xxxx-2	xxxx-3	xxx-3	xxxx-2	xxxx-12	xxx-xxxxx
Monday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Machine/ Thursday Number	xxxxxx	xxx-2	xxx-4	xxxx-1	xxxx-2	xxxx-3	xxx-3	xxxx-2	xxxx-12	xxx-xxxxx
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Special	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Off-site storage

Once a week a set of tapes is sent off-site in case a situation arises in which the systems and their back-up tapes kept at <Site 1> are damaged, destroyed or otherwise put beyond use.

The set of tapes that is sent off-site is the latest Thursday night set. They are collected each Friday morning around 11am, when the previous week's Thursday set of back-ups are returned.

The member of staff who hands the tapes over and receives the set returning must be a recognised signatory for the process. He or she must sign the form and return it to the Helpdesk – having written the number of the set sent off-site on it. The returning set of tapes must be placed in the fire-safe with the other sets.

The company who provides off-site storage for the Trust is:

XX
 XXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXX

'phone: xxxx xxx xxxx.

Document No. ISMS/IBU/AP6	IT Operations Information Backup	
------------------------------	---	--

Appendix 6: Tape Change Log (TCL)

As sample of the form is attached to, and is part of, this Appendix.

How to fill in the Tape Change Log (TCL).

1 On a day when all tapes put in for that night's back-up are the "normal" tapes just tick the "Full Set" column for that day (this will be the usual occurrence).

2 On a day when a different tape to the "normal" tape is used in a machine tick the "New tape?" column for that day (leaving the "Full set" column empty). In the column for the tape concerned record the tape's name as on the label – so that it can identified at a later date if necessary). Tick each column for the tapes where "normal" tapes are used.

3 Thursday tapes are sent off-site on the Friday morning. In the "Set number" record the number of the Thursday set used. In "Comments & Notes" tick "Sent" when sent to Recall & (a week later) tick "Back" when that tape set is returned. The collector from Recall must either sign one of their blue forms OR fill in the relevant part of TCL6 with name, signature, date and details of cases sent and returned.

4 If the "Special" set is used, record this in the "Comments & Notes" column.

5 The entry for a day should be completed by one of the IT Operations staff who did the change. They should record their initials in the "Comments & Notes" column.

6 Record the Monday date for each week in the "Week commencing" box at the top of the form.

7 Record if air conditioning units are working ("tick" for OK "X" for not OK.)

8 Record any back-ups not run in "Comments & Notes".

9 Any other relevant information should be recorded in the "General Comments & Notes" box.

10 If cleaning of the Computer Room & Video conference room take s place during a particular week (usually the week with the 1st of the month in) the the relevant boxes should be ticked.

11 The log forms should be kept for 1 year. A disposal session should be held at least every 3 months to dispose of sheets over 1 year old.

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

Appendix 6: Tape Change Log (TCL)

Appendix 7: xxxxxx backup

(**Note:** To start MVTerm, if not running, click on the MVTerm icon;
from Session go to to mvBASE Server energy 1 inc 0

The above note may not be complete!)

To start backup

Use screen opposite door.

Click on mouse to “wake up” monitor.

If red “Select” light is not on “7” then use “+” or “-“ to move red “Select” light to the “Select” light by 7.
This is the Energy machine.

On the terminal (in mvBASE Virtual Terminal):

1 Put the CAPS LOCK on.

2 At logon type:

SYSPROG [Return]

3 At prompt type the following commands:

T-SELECT 04 [Return]

T-ONLINE [Return]

T-ATT [Return]

FILE-SAVE [Return]

4 At prompts:

STATS REQUIRED? type “N” [Return]

LISTING ? type “N” [Return]

VERIFICATION ? On Monday to Thursdays type “N” [Return]

On FRIDAYS:

Type “Y” [RETURN]

After 40 minutes (approx.) type “Y”
at prompt.

5 The backup is completed when the system logs off and requests the user to log on.
This is about 1 hour after it is started.

The tape for the next day can then be changed.

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

Appendix 8A: To run the daily checks on the XXX XXXXX

Check backup mail messages, type:

```
>su [Return]
Password:
>mail [Return]
```

Output is as shown (& highlighted) in Appendix 8A(3).

There is a script file in usr/users/pireland called start_checks.txt.
To run it, at prompt, type:

```
nhs_supplies > start_checks.txt [Return]
```

This will provide the following output (this has been annotated to show where it matches the check form):

EXAMPLE OUTPUT:

```
nhs_supplies > start_checks.txt
vdumpdates
-----
usr_domain#usr 0 Fri Aug 13 01:38:46 1999
xxxxx_domain#xxxxx 0 Fri Aug 13 01:51:18 1999
root_domain#root 0 Fri Aug 13 02:35:53 1999
indexes_domain#indexes 0 Fri Aug 13 02:08:49 1999
xxxx_domain#datafiles 0 Fri Aug 13 01:15:03 1999
xxxxxxx_domain#xxxxx2 0 Fri Aug 13 02:13:53 1999
xxxxxxx_domain#xxxxx3 0 Fri Aug 13 02:24:29 1999
xxxxxxx_domain#xxxxx4 0 Fri Aug 13 02:36:28 1999
xxxxxxx#xxxxxxx 0 Fri Aug 13 01:29:06 1999
xxxxxxx_domain#xxxxx6 0 Fri Aug 13 02:47:51 1999
bfd_domain#bfd 0 Fri Aug 13 02:55:30 1999
xxxx_domain#SUN2 0 Fri Aug 13 03:37:07 1999

Dbshut log (/u01/stockdata/BACKUPS/dbshut.log)
-----
-rw-r--r-- 1 xxxxx7 dba      500 Aug 13 01:11 /u01/stockdata/BACKUPS/dbg
No SQL*DBA or svrmgrl found in /u01/app/xxxxx/product/7.3.4
Database "ACCM" shut down.
```

Xxxxx Server Manager Release 2.3.4.0.0 - Production

Copyright (c) Xxxxx Corporation 1994, 1995. All rights reserved.

Xxxxx7 Server Release 7.3.4.3.0 with the 64-bit option - Production

With the distributed option
PL/SQL Release 2.3.4.3.0 - Production

```
SVRMGR> Connected.  
SVRMGR> Database closed.  
Database dismounted.  
XXXXX instance shut down.  
SVRMGR>  
Server Manager complete.  
Database "stock" shut down.
```

Dbstart log (/u01/stockdata/BACKUPS/dbstart.log)

```
-----  
-rw-r--r-- 1 xxxxx7 dba      728 Aug 13 07:00 /u01/stockdata/BACKUPS/dbg
```

Can't find init file for Database "ACCM".
Database "ACCM" NOT started.

Xxxxx Server Manager Release 2.3.4.0.0 - Production

Copyright (c) Xxxxx Corporation 1994, 1995. All rights reserved.

Xxxxx7 Server Release 7.3.4.3.0 with the 64-bit option - Production
With the distributed option
PL/SQL Release 2.3.4.3.0 - Production

```
SVRMGR> Connected to an idle instance.  
SVRMGR> XXXXX instance started.  
Total System Global Area  188432192 bytes  
Fixed Size                 50832 bytes  
Variable Size             57145520 bytes  
Database Buffers          131072000 bytes  
Redo Buffers               163840 bytes  
Database mounted.  
Database opened.  
SVRMGR>  
Server Manager complete.
```

Database "stock" warm started.

Xxxxx database alert

```
-----  
cd /bfd/app/xxxxx/product/7.3.4/rdbms/log  
control_files      = /u01/oradata/stock/ctrl1stock.ctl, /u01/oradata/stl  
compatible        = 7.3.2.3.0  
log_buffer         = 163840  
log_checkpoint_interval = 20481  
db_files           = 99
```


Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

```

checkpoint_process      = TRUE
rollback_segments      = r01, r02, r03, r04
sequence_cache_entries = 100
sequence_cache_hash_buckets= 89
max_enabled_roles      = 35
remote_login_passwordfile= NONE
mts_service            = stock
mts_servers            = 0
mts_max_servers        = 0
mts_max_dispatchers    = 0
audit_trail           = NONE
sort_area_size        = 4194304
sort_area_retained_size = 4194304
sort_direct_writes    = TRUE
db_name               = stock
open_cursors          = 255
ifile                 = /bfd/app/xxxxx/product/7.3.4/dbs/configstock.ora
optimizer_mode        = RULE
session_cached_cursors = 150
text_enable           = TRUE
utl_file_dir          = *, /tmp, /u01/home/xxxxx7/acceptance/tmp
shadow_core_dump      = PARTIAL
background_core_dump  = PARTIAL
background_dump_dest  = /bfd/app/xxxxx/product/7.3.4/rdbms/log
user_dump_dest        = /bfd/app/xxxxx/product/7.3.4/rdbms/log
core_dump_dest        = /bfd/app/xxxxx/product/7.3.4/dbs

```

```

PMON started
DBWR started
LGWR started
CKPT started
RECO started
Thu Aug 12 07:00:09 1999
alter database mount exclusive
Thu Aug 12 07:00:10 1999
Successful mount of redo thread 1.
Thu Aug 12 07:00:10 1999
Completed: alter database mount exclusive
Thu Aug 12 07:00:10 1999
alter database open
Beginning crash recovery of 1 threads
Recovery of Online Redo Log: Thread 1 Group 3 Seq 32411 <Site 1> mem 0
  Mem# 0 errs 0: /u01/oradata/stock/log3stock.dbf
Thu Aug 12 07:00:39 1999
Crash recovery completed successfully
Thu Aug 12 07:00:40 1999
Thread 1 advanced to log sequence 32412
  Current log# 4 seq# 32412 mem# 0: /u01/oradata/stock/log4stock.dbf
Thread 1 opened at log sequence 32412
  Current log# 4 seq# 32412 mem# 0: /u01/oradata/stock/log4stock.dbf
Successful open of redo thread 1.

```

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

Thu Aug 12 07:00:45 1999
SMON: enabling cache recovery
Thu Aug 12 07:00:48 1999
Completed: alter database open
Thu Aug 12 07:00:48 1999
SMON: enabling tx recovery
Thu Aug 12 13:56:07 1999
Thread 1 advanced to log sequence 32413
Current log# 1 seq# 32413 mem# 0: /u01/oradata/stock/log1stock.dbf
Thu Aug 12 15:44:04 1999
Thread 1 advanced to log sequence 32414
Current log# 2 seq# 32414 mem# 0: /u01/oradata/stock/log2stock.dbf
Thu Aug 12 16:48:59 1999
Thread 1 advanced to log sequence 32415
Current log# 3 seq# 32415 mem# 0: /u01/oradata/stock/log3stock.dbf
Fri Aug 13 01:11:04 1999
Shutting down instance (normal)
License high water mark = 50
Fri Aug 13 01:11:08 1999
ALTER DATABASE CLOSE NORMAL
Fri Aug 13 01:11:14 1999
SMON: disabling tx recovery
SMON: disabling cache recovery
Fri Aug 13 01:11:31 1999
Thread 1 closed at log sequence 32415
Current log# 3 seq# 32415 mem# 0: /u01/oradata/stock/log3stock.dbf
Fri Aug 13 01:11:33 1999
Completed: ALTER DATABASE CLOSE NORMAL
Fri Aug 13 01:11:33 1999
ALTER DATABASE DISMOUNT
Completed: ALTER DATABASE DISMOUNT
Fri Aug 13 07:00:06 1999
Starting XXXXX instance (normal)
LICENSE_MAX_SESSION = 0
LICENSE_SESSIONS_WARNING = 0
LICENSE_MAX_USERS = 0
Starting up XXXXX RDBMS Version: 7.3.4.3.0.
System parameters with non-default values:
processes = 200
event = 10262 trace name context forever, level 2500
shared_pool_size = 36000000
control_files = /u01/oradata/stock/ctrl1stock.ctl, /u01/oradata/stl
compatible = 7.3.2.3.0
log_buffer = 163840
log_checkpoint_interval = 20481
db_files = 99
checkpoint_process = TRUE
rollback_segments = r01, r02, r03, r04
sequence_cache_entries = 100
sequence_cache_hash_buckets= 89

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

```

max_enabled_roles      = 35
remote_login_passwordfile= NONE
mts_service           = stock
mts_servers           = 0
mts_max_servers       = 0
mts_max_dispatchers    = 0
audit_trail           = NONE
sort_area_size        = 4194304
sort_area_retained_size = 4194304
sort_direct_writes    = TRUE
db_name               = stock
open_cursors          = 255
ifile                 = /bfd/app/xxxxx/product/7.3.4/dbs/configstock.ora
optimizer_mode        = RULE
session_cached_cursors = 150
text_enable           = TRUE
utl_file_dir          = *, /tmp, /u01/home/xxxxx7/acceptance/tmp
shadow_core_dump      = PARTIAL
background_core_dump  = PARTIAL
background_dump_dest  = /bfd/app/xxxxx/product/7.3.4/rdbms/log
user_dump_dest        = /bfd/app/xxxxx/product/7.3.4/rdbms/log
core_dump_dest        = /bfd/app/xxxxx/product/7.3.4/dbs
PMON started
DBWR started
LGWR started
CKPT started
RECO started
Fri Aug 13 07:00:10 1999
alter database mount exclusive
Fri Aug 13 07:00:10 1999
Successful mount of redo thread 1.
Fri Aug 13 07:00:10 1999
Completed: alter database mount exclusive
Fri Aug 13 07:00:10 1999
alter database open
Fri Aug 13 07:00:19 1999
Thread 1 opened at log sequence 32415
  Current log# 3 seq# 32415 mem# 0: /u01/oradata/stock/log3stock.dbf
Successful open of redo thread 1.
Fri Aug 13 07:00:19 1999
SMON: enabling cache recovery
Fri Aug 13 07:00:22 1999
Completed: alter database open
Fri Aug 13 07:00:22 1999
SMON: enabling tx recovery

```

Disk storage

Filesystem	1024-blocks	Used	Available	Capacity	Mounted on
root_domain#root	131072	60413	63736	49%	/

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

```

/proc          0      0      0 100% /proc
usr_domain#usr      893952  802078  59520 94% /usr
xxxxxx_domain#tmp   2055240  29396  255600 11% /tmp
xxxxxx_domain#xxxxx 2055240 1771396 255600 88% /u01
indexes_domain#indexes 895048  675936  212976 77% /indexes
data_domain#datafiles 2055240 1367228 673464 67% /datafiles
xxxxxxxx#xxxxxxxx 2095016 1155863 925864 56% /datafilese
xxxxxxxx_domain#xxxxxxxx 1684824 1433752 245600 86% /xxxxx2
xxxxxxxx_domain#xxxxxxxx 2055240 1483292 562048 73% /xxxxx3
xxxxxxxx_domain#xxxxxxxx 2055240 1894544 154792 93% /xxxxx4
xxxxxxxx_domain#xxxxxxxx 2055240 1509720 538296 74% /xxxxx6
xxxx_domain#xxxx 6000000 2012736 3974912 34% /SUNACCTS
bfd_domain#bfd 11782536 6458618 5287040 55% /bfd

```

Core/Null files

LIVE FORMS - /bfd/production

```

-rw----- 1 jedwards users 3170304 Aug 12 13:08 core
-rw-r--r-- 1 rhodson system 0 Jul 28 16:29 null

```

LIVE REPORTS - /bfd/production/reports

core not found
null not found

TEST FORMS - /bfd/test/forms

core not found
null not found

TEST REPORTS - /bfd/test/reports

core not found
null not found

cd cd /bfd/app/xxxxx/product/7.3.4/dbs

core not found
null not found

core directories

```

total 101
-rw-r----- 1 root dba 819 Mar 27 15:28 configaccm.ora
-rw-r----- 1 root dba 930 Mar 27 15:28 configstock.ora
-rw-r--r-- 1 xxxxx7 dba 7530 Nov 17 1997 init.ora
-rw-r--r-- 1 root dba 4669 Mar 27 15:30 initACCM.ora
-rw-r--r-- 1 xxxxx7 dba 5460 Mar 30 09:28 initstock.bk

```

```
-rw-r--r-- 1 xxxxx7 dba      5504 Jul 29 12:52 initstock.ora
--w--w---- 1 xxxxx7 dba          0 Mar 28 08:57 lkACCM
--w--w---- 1 xxxxx7 dba          0 Mar 27 17:24 lkSTOCK
-rw-r----- 1 xxxxx7 dba      784 Mar 28 10:46 sgadefACCM.dbf
-rw-r----- 1 xxxxx7 dba      784 Aug 13 07:00 sgadefstock.dbf
-rw-r--r-- 1 xxxxx7 dba     73535 Nov 17 1997 sql.bsq
```

Trace files

```
cd /bfd/app/xxxxx/product/7.3.4/rdbms/log
-rw-r----- 1 xxxxx7 dba      5319 Aug 12 06:58 ora_3890.trc
```

remember to do these commands under account su
as these cannot be run from the script

```
tail -40 /usr/var/adm/messages
/usr/users/pireland/dba: No such file or directory
nhs_supplies >
```

(To check whether d/b shutdown for copy [& re-started OK!] check that alert_stock.log
(above) has highlighted items present.)

To run unix messages (see last 5 lines above)

```
nhs_supplies > su
Password:
#
```

```
>tail -40 /usr/var/adm/messages [Return]
```

Enterprise Manager checks for tablespaces & performance

To check tablespaces & Performance Manager overview:

Logon to NT.

Start up Enterprise Manager. At password prompt type:

```
enterprise [TAB]
<password>[TAB]
stock[TAB]
```

For Tablespace Manager:

From "Main Screen" select "Tools" from menu bar.

Select Tablespace Manager from popup.

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

At password prompt type:

```
enterprise [TAB]
<password>[TAB]
stock[TAB]
```

At main "tree" select tablespaces & note % free space.

Leave tablespace manager.

For Performance Manager Overview:

From "Main Screen" select "Tools" from menu bar.

Select Performance Manager from popup.

At password prompt type:

```
enterprise [TAB]
<password>[TAB]
stock[TAB]
```

Select Display Overview and note items on form.

Exit Performance Manager & Enterprise Manager.

Appendices

8A(1) Text of "start_checks.txt" – the daily checks routine

```
nhs_supplies > view start_checks.txt
"start_checks.txt" [Read only] 76 lines, 1823 characters
echo "vdumpdates"
echo "-----"
cat /etc/vdumpdates
echo
echo "Dbshut log (/u01/stockdata/BACKUPS/dbshut.log)"
echo "-----"
ls -la /u01/stockdata/BACKUPS/dbshut.log
cat /u01/stockdata/BACKUPS/dbshut.log
echo
echo
echo "Dbstart log (/u01/stockdata/BACKUPS/dbstart.log)"
echo "-----"
ls -la /u01/stockdata/BACKUPS/dbstart.log
cat /u01/stockdata/BACKUPS/dbstart.log
echo
```

```
echo
echo "xxxxxx database alert"
echo "-----"
cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log
echo "cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log"
tail -150 alert_stock.log
echo
echo "Disk storage"
echo "-----"
df -kx
echo
echo "Core/Null files"
echo "-----"
echo
echo "LIVE FORMS - /bfd/production"
echo "-----"
cd /bfd/production
ls -l core
ls -l null
echo
echo "LIVE REPORTS - /bfd/production/reports"
echo "-----"
cd /bfd/production/reports
ls -l core
ls -l null
echo
echo "TEST FORMS - /bfd/test/forms"
echo "-----"
cd /bfd/test/forms
ls -l core
ls -l null
echo
echo "TEST REPORTS - /bfd/test/reports"
echo "-----"
cd /bfd/test/reports
ls -l core
ls -l null
echo
echo "vdumpdates"
echo "-----"
cat /etc/vdumpdates
echo
echo "Dbshut log (/u01/stockdata/BACKUPS/dbshut.log)"
echo "-----"
ls -la /u01/stockdata/BACKUPS/dbshut.log
cat /u01/stockdata/BACKUPS/dbshut.log
echo
echo
echo "Dbstart log (/u01/stockdata/BACKUPS/dbstart.log)"
echo "-----"
```

```
ls -la /u01/stockdata/BACKUPS/dbstart.log
cat /u01/stockdata/BACKUPS/dbstart.log
echo
echo
echo "xxxxxx database alert"
echo "-----"
cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log
echo "cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log"
tail -150 alert_stock.log
echo
echo "Disk storage"
:q!
nhs_supplies > tail -200 start_checks.txt
echo "vdumpdates"
echo "-----"
cat /etc/vdumpdates
echo
echo "Dbshut log (/u01/stockdata/BACKUPS/dbshut.log)"
echo "-----"
ls -la /u01/stockdata/BACKUPS/dbshut.log
cat /u01/stockdata/BACKUPS/dbshut.log
echo
echo
echo "Dbstart log (/u01/stockdata/BACKUPS/dbstart.log)"
echo "-----"
ls -la /u01/stockdata/BACKUPS/dbstart.log
cat /u01/stockdata/BACKUPS/dbstart.log
echo
echo
echo "Xxxxx database alert"
echo "-----"
cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log
echo "cd /bfd/app/xxxxxx/product/7.3.4/rdbms/log"
tail -150 alert_stock.log
echo
echo "Disk storage"
echo "-----"
df -k
echo
echo "Core/Null files"
echo "-----"
echo
echo "LIVE FORMS - /bfd/production"
echo "-----"
cd /bfd/production
ls -l core
ls -l null
echo
echo "LIVE REPORTS - /bfd/production/reports"
echo "-----"
```



```
cd /bfd/production/reports
ls -l core
ls -l null
echo
echo "TEST FORMS - /bfd/test/forms"
echo "-----"
cd /bfd/test/forms
ls -l core
ls -l null
echo
echo "TEST REPORTS - /bfd/test/reports"
echo "-----"
cd /bfd/test/reports
ls -l core
ls -l null
echo
echo "cd cd /bfd/app/xxxxx/product/7.3.4/dbs"
echo "-----"
cd /bfd/app/xxxxx/product/7.3.4/dbs
ls -l core
ls -l null
echo
echo "core directories"
echo "-----"
ls -lR
echo
echo "Trace files"
echo "-----"
echo "cd /bfd/app/xxxxx/product/7.3.4/rdbms/log"
cd /bfd/app/xxxxx/product/7.3.4/rdbms/log
ls -lrt *.trc
echo
echo
echo
echo "remember to do these commands under account su"
echo "as these cannot be run from the script"
echo "-----"
echo "tail -40 /usr/var/adm/messages"
cd $HOME/dba
nhs_supplies >
```

8A(2) See also attached "original" list of checks for reference:

Everyday Tasks

Backup Procedure Checks

1 Logon as <user name>

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

2 At prompt type:

```
> su [R]
password
```

```
>mail [R]
```

to read messages.

Count tape "rewind" messages (there should be four).
Check that each file domain has reached 100% backup.)

Backup is OK if messages are of type:

```
vdump: Dumped etc
all the way down.
```

To quit mail:

```
at ? prompt
q[R]
```

```
# exit [R] (to leave "superuser")
```

[Saturdays & Sundays there are 2 back-ups, one Saturday am & one Sunday am. To get to mail about these press [RETURN] at '?' prompt (in mail) to see previous messages. First message is "rm:/u01/stockdata/BACKUPS/dbshut.log: No such file or directory". (This is OK.) 3rd message (between 2 "back_up mail" messages is: "find:bad_status -- /tmp/croutVEFaaaqEa" is OK too!]

```
> cat /etc/vdumpdates[R]
```

3 Check Xxxxx d/b alert_ (check more than once a day)

```
> cd $XXXXXX_HOME/./7.3.2/rdbms/log [R]
(maps to /u01/app/xxxxx/product/7.3.2/rdbms/log)
```

```
> tail -150 alert_stock.log [R]
```

[On Mondays use:

```
> tail -650 alert_stock.log[R]
```

to get back to Friday start (the value -650 may need to be changed if Friday start can't be reached).]

Look for error or alert messages (eg ORA-1652)

Check for abnormal messages which we can do anything about.

4 Disk Storage

Command: df -k

Under <user name> user type

```
> df -k
```

Lists unix filesystems on system & their sizes in megabyte blocks.

The two of interest are: /tmp (sorting data area etc) and /u01. u01 should be between 85% & 93% (if 100% then /tmp is likely to be 100% too - check too see if there are core dump files and remove if any. Also check for null files and remove if large).

Core & null files are in:

```
>cd $ACCEPT (to /u01/home/xxxxx7/acceptance)
```

```
>ls -l core [R]
```

```
>ls -l null [R]
```

```
>cd $FORMS
```

```
>ls -l core[R]
```

```
>ls -l null [R]
```

```
>cd $REPORTS
```

```
>ls -l core[R]
```

```
>ls -l null [R]
```

```
>cd $XXXXX_HOME/./7.3.2/dbs  
(to /u01/app/xxxxx/product/7.3.2/dbs)
```

```
>ls -l core [R]
```

```
>ls -l null [R]
```

[To remove core & null files (if found above):

```
>rm core[R]
```

or

```
>rm null[R]
```

].

```
> ls -lR[R] (ie list core sub-directories too)
```

If core files are shown then:

```
>cd coreX (where X = no. of directories)
```

```
>rm <core file name>
```

To remove core directories

```
>su [R] (to be superuser)  
<password>
```

```
# rmdir core_* [R]
```

Check trace files

These are in /u01/app/xxxxx/product/./7.3.2/rdbms/log

```
> cd $XXXXX_HOME/7.3.2/rdbms/log [R]  
(maps to /u01/app/xxxxx/product/7.3.2/rdbms/log)
```

```
> ls -lrt *.trc (gives list of trace files)
```

(To remove trace files:

```
>su[R]  
<password>
```

```
#rm *.trc[R]
```

```
#exit[R] ).
```

5 Check Unix System Messages file

```
>su [R]  
<password>
```

```
# tail -40 /usr/var/adm/messages[R]
```

Check these a few times a day.

```
#exit[R].
```

6 To use Enterprise Manager

To check tablespaces & Performance Manager overview:

Logon to NT.

Start up Enterprise Manager. At password prompt type:

```
enterprise [TAB]  
<password>[TAB]  
stock[TAB]
```

For Tablespace Manager:

From "Main Screen" select "Tools" from menu bar.

Select Tablespace Manager from popup.

At password prompt type:

enterprise [TAB]
<password>[TAB]
stock[TAB]

At main "tree" select tablespaces & note % free space.

Leave tablespace manager.

For Performance Manager Overview:

From "Main Screen" select "Tools" from menu bar.

Select Performance Manager from popup.

At password prompt type:

enterprise [TAB]
<password>[TAB]
stock[TAB]

Select Display Overview and note items on form.

Exit Performance Manager & Enterprise Manager.

8A(3) Backup mail messages – example

?

From root Sat Aug 14 03:44:42 1999
Received: by nhssadec1.supplies.nhs.uk id AA25902; Sat, 14 Aug 1999 03:44:41 +00
Date: Sat, 14 Aug 1999 03:44:41 +0100
From: system PRIVILEGED account <root>
Message-Id: <199908140244.AA25902@nhssadec1.supplies.nhs.uk>
Apparently-To: root

path : /datafiles
dev/fset : data_domain#datafiles
type : advfs
advfs id : 0x2ffbd2f0.00078180.2
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1399927296 bytes, 8 directories, 19 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 01:21:02 1999
vdump: Dumped 629190656 of 1399927296 bytes; 44.9% completed
vdump: Dumped 2 of 8 directories; 25.0% completed
vdump: Dumped 4 of 19 files; 21.1% completed

vdump: Status at Sat Aug 14 01:26:39 1999

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

vdump: Dumped 1295060820 of 1399927296 bytes; 92.5% completed
vdump: Dumped 7 of 8 directories; 87.5% completed
vdump: Dumped 15 of 19 files; 78.9% completed

vdump: Status at Sat Aug 14 01:27:42 1999
vdump: Dumped 1399927296 of 1399927296 bytes; 100.0% completed
vdump: Dumped 8 of 8 directories; 100.0% completed
vdump: Dumped 19 of 19 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 01:27:42 1999
path : /datafiles/britcave
dev/fset : xxxxxxxxxxxx#xxxxxxxxxxxxxx
type : advfs
advfs id : 0x33d39f49.000e1a70.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1163607867 bytes, 1784 directories, 6905 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 01:34:11 1999
vdump: Dumped 497299754 of 1163607867 bytes; 42.7% completed
vdump: Dumped 1704 of 1784 directories; 95.5% completed
vdump: Dumped 2083 of 6905 files; 30.2% completed

vdump: Status at Sat Aug 14 01:38:55 1999
vdump: Dumped 1163607867 of 1163607867 bytes; 100.0% completed
vdump: Dumped 1784 of 1784 directories; 100.0% completed
vdump: Dumped 6905 of 6905 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 01:38:55 1999
path : /usr
dev/fset : usr_domain#usr
type : advfs
advfs id : 0x2fa4f089.00085700.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 840861328 bytes, 1887 directories, 34362 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 01:45:38 1999
vdump: Dumped 477138138 of 840861328 bytes; 56.7% completed
vdump: Dumped 518 of 1887 directories; 27.5% completed
vdump: Dumped 10671 of 34362 files; 31.1% completed

vdump: Status at Sat Aug 14 01:50:38 1999
vdump: Dumped 803268602 of 840861328 bytes; 95.5% completed
vdump: Dumped 1423 of 1887 directories; 75.4% completed
vdump: Dumped 31181 of 34362 files; 90.7% completed

vdump: Status at Sat Aug 14 01:51:20 1999
vdump: Dumped 840861679 of 840861328 bytes; 100.0% completed
vdump: Dumped 1887 of 1887 directories; 100.0% completed

vdump: Dumped 34362 of 34362 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 01:51:20 1999
path : /u01
dev/fset : xxxxx_domain#xxxxx
type : advfs
advfs id : 0x2fb74077.000423e0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1976773597 bytes, 611 directories, 11991 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 01:57:04 1999
vdump: Dumped 777633946 of 1976773597 bytes; 39.3% completed
vdump: Dumped 323 of 611 directories; 52.9% completed
vdump: Dumped 3637 of 11991 files; 30.3% completed

vdump: Status at Sat Aug 14 02:02:08 1999
vdump: Dumped 1419824738 of 1976773597 bytes; 71.8% completed
vdump: Dumped 531 of 611 directories; 86.9% completed
vdump: Dumped 7056 of 11991 files; 58.8% completed

vdump: Status at Sat Aug 14 02:07:52 1999
vdump: Dumped 1903700511 of 1976773597 bytes; 96.3% completed
vdump: Dumped 593 of 611 directories; 97.1% completed
vdump: Dumped 11423 of 11991 files; 95.3% completed

vdump: Status at Sat Aug 14 02:08:45 1999
vdump: Dumped 1976773597 of 1976773597 bytes; 100.0% completed
vdump: Dumped 611 of 611 directories; 100.0% completed
vdump: Dumped 11991 of 11991 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:08:45 1999
path : /indexes
dev/fset : indexes_domain#indexes
type : advfs
advfs id : 0x2ffa70d1.000215c0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 692090880 bytes, 4 directories, 9 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:13:42 1999
vdump: Dumped 692090880 of 692090880 bytes; 100.0% completed
vdump: Dumped 4 of 4 directories; 100.0% completed
vdump: Dumped 9 of 9 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:13:42 1999
path : /xxxxx2
dev/fset : xxxxx2_domain#xxxxx2
type : advfs
advfs id : 0x31d79440.00006ac0.1
vdump: Date of last level 0 dump: the start of the epoch

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

vdump: Dumping directories
vdump: Dumping 1468055552 bytes, 6 directories, 14 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:18:50 1999
vdump: Dumped 1048614912 of 1468055552 bytes; 71.4% completed
vdump: Dumped 5 of 6 directories; 83.3% completed
vdump: Dumped 9 of 14 files; 64.3% completed

vdump: Status at Sat Aug 14 02:20:47 1999
vdump: Dumped 1468055552 of 1468055552 bytes; 100.0% completed
vdump: Dumped 6 of 6 directories; 100.0% completed
vdump: Dumped 14 of 14 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:20:47 1999

path : /xxxxx3
dev/fset : xxxxx3_domain#xxxxx3
type : advfs
advfs id : 0x33d39ba4.00033b50.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1513143534 bytes, 43 directories, 6251 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:26:02 1999
vdump: Dumped 859887616 of 1513143534 bytes; 56.8% completed
vdump: Dumped 2 of 43 directories; 4.7% completed
vdump: Dumped 9 of 6251 files; 0.1% completed

vdump: Status at Sat Aug 14 02:30:26 1999
vdump: Dumped 1513143534 of 1513143534 bytes; 100.0% completed
vdump: Dumped 43 of 43 directories; 100.0% completed
vdump: Dumped 6251 of 6251 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:30:26 1999

path : /
dev/fset : root_domain#root
type : advfs
advfs id : 0x36fb8e4a.000e8cd0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 62674389 bytes, 153 directories, 3102 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:31:01 1999
vdump: Dumped 62674389 of 62674389 bytes; 100.0% completed
vdump: Dumped 153 of 153 directories; 100.0% completed
vdump: Dumped 3102 of 3102 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:31:01 1999
path : /xxxxx4
dev/fset : xxxxx4_domain#xxxxx4
type : advfs

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

advfs id : 0x351cff66.0000e4c0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1939929088 bytes, 2 directories, 17 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:36:30 1999
vdump: Dumped 943761408 of 1939929088 bytes; 48.6% completed
vdump: Dumped 2 of 2 directories; 100.0% completed
vdump: Dumped 7 of 17 files; 41.2% completed

vdump: Status at Sat Aug 14 02:41:48 1999
vdump: Dumped 1835069440 of 1939929088 bytes; 94.6% completed
vdump: Dumped 2 of 2 directories; 100.0% completed
vdump: Dumped 16 of 17 files; 94.1% completed

vdump: Status at Sat Aug 14 02:42:23 1999
vdump: Dumped 1939929088 of 1939929088 bytes; 100.0% completed
vdump: Dumped 2 of 2 directories; 100.0% completed
vdump: Dumped 17 of 17 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:42:23 1999
path : /xxxxx6

dev/fset : xxxxx6_domain#xxxxx6
type : advfs
advfs id : 0x348eb8c5.000d1360.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 1543032864 bytes, 125 directories, 2304 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:48:48 1999
vdump: Dumped 1302813715 of 1543032864 bytes; 84.4% completed
vdump: Dumped 21 of 125 directories; 16.8% completed
vdump: Dumped 1009 of 2304 files; 43.8% completed

vdump: Status at Sat Aug 14 02:50:03 1999
vdump: Dumped 1543032864 of 1543032864 bytes; 100.0% completed
vdump: Dumped 125 of 125 directories; 100.0% completed
vdump: Dumped 2304 of 2304 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 02:50:03 1999
path : /bfd

dev/fset : bfd_domain#bfd
type : advfs
advfs id : 0x36babf74.000a92e0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories
vdump: Dumping 7120719786 bytes, 1154 directories, 51833 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 02:56:24 1999

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

vdump: Dumped 1057271078 of 7120719786 bytes; 14.8% completed
vdump: Dumped 268 of 1154 directories; 23.2% completed
vdump: Dumped 23878 of 51833 files; 46.1% completed

vdump: Status at Sat Aug 14 03:01:26 1999
vdump: Dumped 1765155101 of 7120719786 bytes; 24.8% completed
vdump: Dumped 674 of 1154 directories; 58.4% completed
vdump: Dumped 30183 of 51833 files; 58.2% completed

vdump: Status at Sat Aug 14 03:06:26 1999
vdump: Dumped 2730139128 of 7120719786 bytes; 38.3% completed
vdump: Dumped 982 of 1154 directories; 85.1% completed
vdump: Dumped 34729 of 51833 files; 67.0% completed

vdump: Status at Sat Aug 14 03:11:26 1999
vdump: Dumped 3545451543 of 7120719786 bytes; 49.8% completed
vdump: Dumped 1022 of 1154 directories; 88.6% completed
vdump: Dumped 36765 of 51833 files; 70.9% completed

vdump: Status at Sat Aug 14 03:16:26 1999
vdump: Dumped 4596471904 of 7120719786 bytes; 64.6% completed
vdump: Dumped 1029 of 1154 directories; 89.2% completed
vdump: Dumped 38035 of 51833 files; 73.4% completed

vdump: Status at Sat Aug 14 03:21:26 1999
vdump: Dumped 5578760531 of 7120719786 bytes; 78.3% completed
vdump: Dumped 1081 of 1154 directories; 93.7% completed
vdump: Dumped 40425 of 51833 files; 78.0% completed

vdump: Status at Sat Aug 14 03:26:26 1999
vdump: Dumped 6277690674 of 7120719786 bytes; 88.2% completed
vdump: Dumped 1098 of 1154 directories; 95.1% completed
vdump: Dumped 46155 of 51833 files; 89.0% completed

vdump: Status at Sat Aug 14 03:31:27 1999
vdump: Dumped 7104773230 of 7120719786 bytes; 99.8% completed
vdump: Dumped 1151 of 1154 directories; 99.7% completed
vdump: Dumped 51750 of 51833 files; 99.8% completed

vdump: Status at Sat Aug 14 03:31:32 1999
vdump: Dumped 7120719786 of 7120719786 bytes; 100.0% completed
vdump: Dumped 1154 of 1154 directories; 100.0% completed
vdump: Dumped 51833 of 51833 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 03:31:32 1999
path : /xxxxxxx
dev/fset : xxxx_domain#SUN2
type : advfs
advfs id : 0x36babf6b.000053e0.1
vdump: Date of last level 0 dump: the start of the epoch
vdump: Dumping directories

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

vdump: Dumping 2052768908 bytes, 524 directories, 6485 files
vdump: Dumping regular files

vdump: Status at Sat Aug 14 03:36:48 1999
vdump: Dumped 953874259 of 2052768908 bytes; 46.5% completed
vdump: Dumped 39 of 524 directories; 7.4% completed
vdump: Dumped 2567 of 6485 files; 39.6% completed

vdump: Status at Sat Aug 14 03:41:50 1999
vdump: Dumped 1844398769 of 2052768908 bytes; 89.8% completed
vdump: Dumped 40 of 524 directories; 7.6% completed
vdump: Dumped 3120 of 6485 files; 48.1% completed
vdump: Rewinding and unloading tape

vdump: Status at Sat Aug 14 03:44:40 1999
vdump: Dumped 2052768908 of 2052768908 bytes; 100.0% completed
vdump: Dumped 524 of 524 directories; 100.0% completed
vdump: Dumped 6485 of 6485 files; 100.0% completed
vdump: Dump completed at Sat Aug 14 03:44:40 1999

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

Appendix 8B: Daily Tasks Check List & Results – XXX XXXXX

Check back-up mail message OK? Y/N
If N note details here & continue overleaf:

	datafiles	usr	U01	indexes	xxxxx 2	Xxxxx 3	/	xxxxx4	xxxxx6	bfd
vdupdate										

Check alert log file OK? Y/N
If N note details here & continue overleaf

--

Check Disk Storage OK? Y/N

/			
proc			
usr			
tmp			
u01			
indexes			
datafiles			
xxxxx 2			
xxxxx 3			
xxxxx 4			
xxxxx 6			
bfd			
cdrom			
sunacct			
datafilese			

Core files
\$ACCEPT
\$FORMS
\$REPORTS
\$XXXXX_HOME/..7.3.2/dbs

Document No. ISMS/IBU/001	IT Operations Information Backup	
------------------------------	---	--

Date:

Check trace files None? Y/N
If N note details here & continue overleaf

Check Unix System Message File OK? Y/N
If N note details here & continue overleaf

Routine Checks through day

Check	10.00	13.15	16.30
df -k			
alert			
unix			

If not OK see notes overleaf

	9.30	1.15	4.30
Acceptance			
enterprisemanager			
new_indexes			
products			
products_indexes			
rbs			
stock_data			
stock_indexes			
system			
temp_users			
tools			
training			
users			

	users logged on	active	Running	memory allocation
9.30				
1.15				
4.30				

**THIS PROCEDURE IS NO LONGER USED – BUT MAY CONTAIN
USEFUL INFO. ESPECIALLY ON RESTORES ETC.**

APPENDIX 9: BACKUP PROCEDURE

Daily Routine

Currently, the backups are looked after by the IT team at <Site 1> where the xxx machine resides.

Four 120m DAT tapes are used for the backup. They are inserted into the tape holder with tape 1 at the top and tape 4 at the bottom.

Each morning the tapes from the previous evening's backup are removed from the xxx and placed in the safe.

Each evening the tapes for that evening's backup are placed in the xxx.

The tapes placed in the safe the previous day are removed from the safe and taken off-site.

Sets of tapes are rotated as follows:

Monday, Tuesday, Wednesday, Thursday, Friday
These tapes are rotated on a weekly basis.

The tapes used on the last day of the month are taken off-site and kept for a month. Their place in the weekly rotation is taken by the tapes kept from the end of the previous month.

The time and date of the start of each filesystem's backup is recorded in the file /etc/vdumpdates.

**THIS PROCEDURE IS NO LONGER USED – BUT MAY CONTAIN
USEFUL INFO. ESPECIALLY ON RESTORES ETC.**

The following is a copy of the backup routine. This routine is stored in
/u01/stockdata/BACKUPS/backup and is run by the root's crontab.

```
/sbin/rm /u01/stockdata/BACKUPS/backup.log
echo Start of Backup > /u01/stockdata/BACKUPS/backup.log

echo Initialising Tape Deck >> /u01/stockdata/BACKUPS/backup.log
/usr/bin/mcutil -l
/usr/bin/mcutil -e >> /u01/stockdata/BACKUPS/backup.log
echo Putting Tape 1 into Drive >> /u01/stockdata/BACKUPS/backup.log
/usr/bin/mcutil -m s:0 d:0
/usr/bin/mcutil -e >> /u01/stockdata/BACKUPS/backup.log

echo Starting vdump >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -N -u -f /dev/rmt0h /datafiles >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -u -f /dev/rmt0h /usr >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -u -f /dev/rmt0h /u01 >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -N -u -f /dev/rmt0h /indexes >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -N -u -f /dev/rmt0h /xxxxx2 >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -N -u -f /dev/rmt0h /xxxxx3 >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump -0 -u -f /dev/rmt0h / >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump/-0 -N -u -f /dev/rmt0h /xxxxx4 >> /u01/stockdata/BACKUPS/backup.log
/sbin/vdump/-0 -u -f /dev/rmt0h /xxxxx6 >> /u01/stockdata/BACKUPS/backup.log

echo Removing Tape from drive >> /u01/stockdata/BACKUPS/backup.log
/usr/bin/mcutil -l
/usr/bin/mcutil -e >> /u01/stockdata/BACKUPS/backup.log
```


NB: The 'N' on some of the lines starting with /sbin/vdump tells the vdump program not to rewind the mounted tape after backing up the directories. Lines without the 'N' will rewind the tape and move onto the next tape. Therefore, if we look at the archive part of the backup crontab, it becomes clearer when the vdump program changes tapes.

```
Tape 1
  /sbin/vdump -0 -N -u -f /dev/rmt0h /datafiles >> /u01/stockdata/BACKUPS/backup.log
  /sbin/vdump -0 -u -f /dev/rmt0h /usr >> /u01/stockdata/BACKUPS/backup.log
Tape 2
  /sbin/vdump -0 -u -f /dev/rmt0h /u01 >> /u01/stockdata/BACKUPS/backup.log
Tape 3
  /sbin/vdump -0 -N -u -f /dev/rmt0h /indexes >> /u01/stockdata/BACKUPS/backup.log
  /sbin/vdump -0 -N -u -f /dev/rmt0h /xxxxx2 >> /u01/stockdata/BACKUPS/backup.log
  /sbin/vdump -0 -N -u -f /dev/rmt0h /xxxxx3 >> /u01/stockdata/BACKUPS/backup.log
  /sbin/vdump -0 -u -f /dev/rmt0h / >> /u01/stockdata/BACKUPS/backup.log
Tape 4
  /sbin/vdump/-0 -N -u -f /dev/rmt0h /xxxxx4 >> /u01/stockdata/BACKUPS/backup.log
  /sbin/vdump/-0 -u -f /dev/rmt0h /xxxxx6 >> /u01/stockdata/BACKUPS/backup.log
```

**THIS PROCEDURE IS NO LONGER USED – BUT MAY CONTAIN
USEFUL INFO. ESPECIALLY ON RESTORES ETC.**

Tape 1: /datafiles and /usr
Tape 2: /u01
Tape 3: /indexes, /xxxxx2, /xxxxx3 and /
Tape 4: /xxxxx4 and /xxxxx6

To restore data from tapes with multiple filesets:

vrestore -t -f /dev/nrmt0h

will list all files in first fileset BUT will not rewind afterwards, thus a further:

vrestore -t -f /dev/nrmt0h

will list all files in second fileset etc.

Notes.

If a tape or the last tape becomes full, there are two things which can be done

- 1. Delete any old or unused data from the relevant directories and disks. Also, make sure that there are no large xxxxx core dumps which take up considerable space themselves.*
- 2. The crontab behind the backup procedure sends mail messages to the superuser account. By looking at the unix mail for superuser and by looking at the free disk space on the drives (df -k), you may be able to move different directory backups onto another tape or arrange them in another combination depending on how much space is left on each tape and the size of the disks. If doing this, it is advisable to put all the xxxxx datafile backup on the first set of tapes so as to avoid a backup of xxxxx datafiles taking place whilst the database is coming back up between 6.45 and 7.00am.*

Appendix 10: Synchronise procedure

The Synchroniser ...

... using “synchronise” to back-up and recover
your lap-top files

What is the “Synchroniser”?

The “Synchroniser” is a piece of software that allows files on your lap-top (or desk-top) pc’s hard-disk to be copied to or synchronised with Cxxxx and vice versa so that your files can be backed-up on Cxxxx or retrieved from Cxxxx.

Some definitions

1 You can use the Synchroniser on your lap-top pc or your desk-top pc - for clarity these instructions will refer only to your lap-top pc – just substitute “desk-top pc” for “lap-top pc” if you want to use these instructions on your desk-top pc.

2 You may know that the area where you store a collection of files in Cxxxx and on your lap-top/desk-top pc by the Windows name of **folder**; other computer systems call this area a **directory**. In these instructions and in the Synchroniser software a **folder** and a **directory** are the same thing and are used inter-changeably.

3 The files and/or directories that you are copying (or synchronising) FROM will be called the **source** files or directories.

4 The files and/or directories that you are copying (or synchronising) TO will be called the **target** files or directories.

What’s the difference between Copying and Synchronising?

Copying a source directory to Cxxxx from your lap-top pc (or the other way round) will copy ALL files in that directory to the target directory on Cxxxx. Similarly ALL files in a source directory on Cxxxx will be copied to the target directory on your lap-top pc.

Synchronising a source directory on your lap-top pc with a target directory on Cxxxx (or the other way round) will make the contents of the target directory EXACTLY the same as the source directory contents. That is, it will update the target directories files with the same versions as those in the source directory, add files that are in the source directory but not in the target directory and DELETE files that are in the target directory but not in the source directory. Therefore the Synchroniser should be used with some caution as you may up-date files that you did not mean to – OR YOU MAY LOSE FILES you did not want to!

How to use the Synchroniser

Initial set-up

The first time you use the Synchroniser there will probably be a lot of work for Cxxxx and your lap-top to do. To save you time and to save money on 'phone bills it is recommended that you do the initial synchronisation of your files via a network link in <Site 1>, or <Site 2>. Subsequent synchronising sessions should be quicker since Cxxxx and your lap-top pc will have done most of the hard-work in the initial set-up session, thus you can use the Synchroniser by normal dial-up link to Cxxxx as it SHOULDN'T take too long.

Starting Synchroniser

From the Cxxxx desk-top click on the following route:

Start > Programs > Accessories > Synchronise. (See Figure 1.)

Figure 1.

The Synchroniser window looks like this:

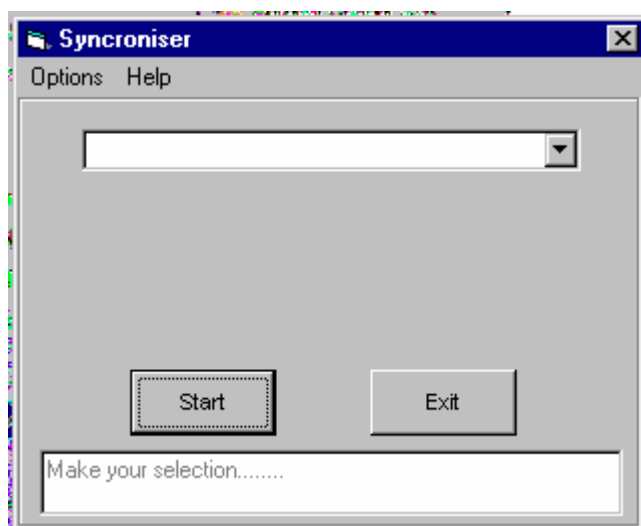
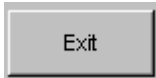




Figure 2.

Exiting Synchroniser



Click  or  (top Right Hand corner of Synchroniser window).

Setting up the Synchroniser so that it works with the directories you want

(this is the start of either the Copying or Synchronising procedure [see below] and must be done each time before Copying or Synchronising files or directories).

- 1 Start Synchroniser as above.
- 2 From the "Synchroniser" window click on the following route:

Options > Drives (see Figure 3)



Figure 3.

and you will be presented with the "Drive Options" window (Figure 4).

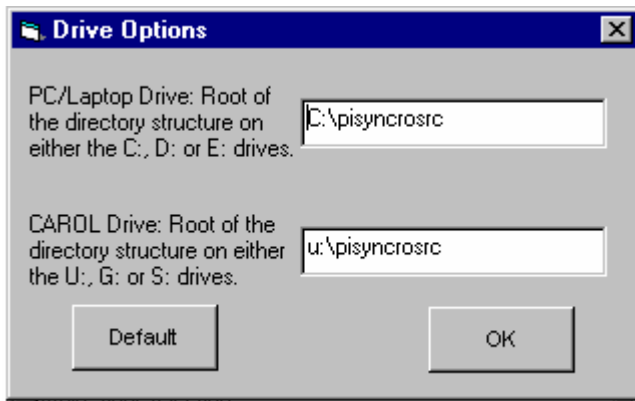


Figure 4.

3 In the "Drive Options" window enter, as follows, the specifications for the Cxxxx & lap-top drives that you are going to work with:

- a) IN THE TOP BOX: the directory and path, on the lap-top pc that you want to copy to or from – the drives to choose from are C: , D: or E: .

The format for the drive & directory path is:

<drive>:\<path>\<directory to back-up or recover>

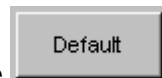
An example:

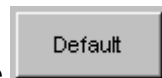
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup

where:

C = <drive>;
Documents and Settings\Administrator\Start Menu\Programs\
= <path> and
Startup = <directory to back-up>

- b) IN THE BOTTOM BOX: the directory and path on Cxxxx that you want to copy from or to – the drives to choose from are U: , G: or S: . See paragraph 3a above for an example of what a drive, path & directory entry for this box should look like.



- c) The  button sets the both drive paths back to C:\synchron (lap-top) and U:\synchron (Cxxxx) – which can be used as designated areas on them for running the Synchroniser.

If the target directory (on either the lap-top or Cxxxx) does not exist then the Synchroniser will create the directory for you before placing files in it.

d) Now perform the Copy or Synchronise operation that you wish – see relevant section, below, on how to perform these procedures.

Copying

1 Set up the drives that you wish to work with (see above section).

2 From the “Synchronise” window click on the  by the top box to see the list of operations (see Figure 5).

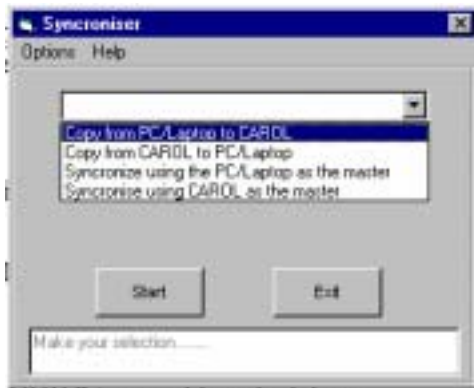


Figure 5.

3 Choose from “Copy from “PC/Laptop to CXXXX” (copies files which have changed or which are new from lap-top to CXXXX; no files are deleted) or “Copy from CXXXX to PC/Laptop” (copies files which are new from CXXXX to your lap-top; no files are deleted).

4 Click the  button.

5 The copy’s progress is displayed in the box at the bottom of the window.

6 At the end of the copy the following message will appear:

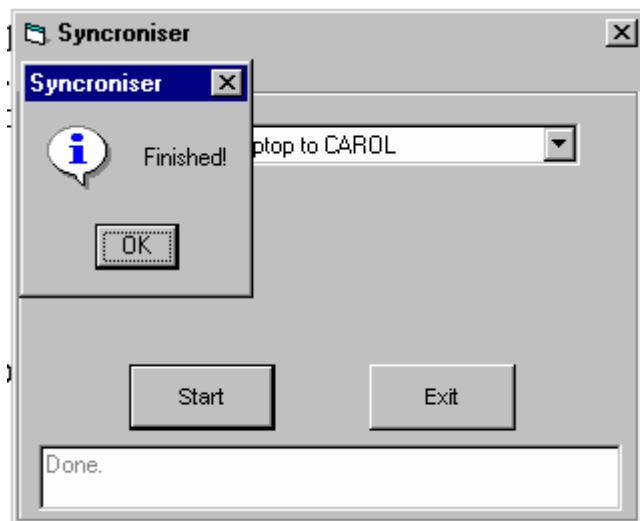


Figure 7.

7 Click OK to return to the front screen to perform further Synchroniser procedures or to exit.

Synchronising

1 Set up the drives that you wish to work with (see above section).


2 From the “Synchronise” window click on the  by the top box to see the list of operations (see Figure 5).



Figure 8.

3 Choose from “Synchronise using the PC/laptop as master” (makes sure that the newest version of existing files are maintained on both systems. Copies new files from your laptop to CXXXX and prompts for the deletion of files which only exist on CXXXX.) or “Synchronise using CXXXX as the master” (makes sure that the newest version of existing files are maintained on both systems. Copies new files from CXXXX to your laptop and prompts for the deletion of files which only exist on your laptop.).

4 Click the  button.

5 The synchronisation’s progress is displayed in the box at the bottom of the window.

6 At the end of the synchronisation the following message will appear (as well as a summary of files synchronised):

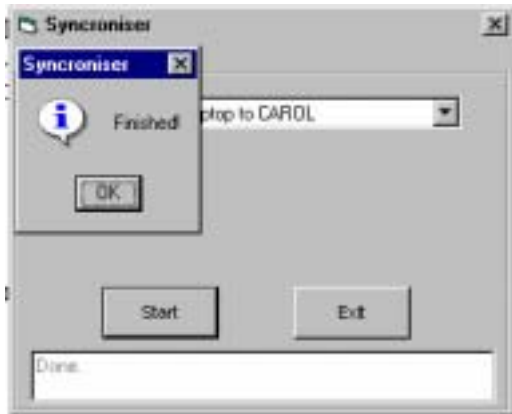


Figure 9.

7 Click OK to return to the front screen to perform further Synchroniser procedures or to exit.

... and remember - you are not alone! Getting help.

If you have any queries or problems with using the Synchroniser contact the IT Helpdesk on (xxxxxxxxxx) xxxx xxxx or (xx) xxxx xxx xxxx.