NATIONAL RIVERS AUTHORITY

THAMES REGION

MICRO COMPUTER GUIDELINES

Author: Tony Slade, Team Leader Small Systems

Date: 6 January 1993

Version: Version 1.00

Project: SP3331

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose of guidelines

The Region has a large number of microcomputers, a significant number of which are connected to Local Area Networks (LANs). Their use is becoming more widespread as power, portability and the availability of suitable software increase. It has therefore become necessary to formulate some guidelines to help users in the day-to-day operation of microcomputers. The aim of this document is to:

- improve the effectiveness of microcomputer usage within the Region;
- reduce the risks associated with such computers;
- promote the efficient use of the Region's computing resources;
- ensure that relevant legislation and technical standards are complied with.

Until there are national standards and procedures, staff in the Region must comply with these guidelines. However, they are not intended to be a definitive judgment on the issues addressed and any questions concerning them should be discussed with the Helpdesk. In particular, this document is undoubtedly no substitute for a technical manual when dealing with detailed practical points.

1.2 Responsibilities of user departments

It is the responsibility of *managers* to ensure that all microcomputer *users* within their section follow the advice given in these guidelines.

Each microcomputer within a department will be allocated to a *'registered user'* who will be responsible for ensuring that the guidelines are complied with in relation to his/her own equipment.

2 ACQUIRING SYSTEMS

2.1 Procedures

The 'Interaction with the IT Group' and 'IT Liaison Group procedures' documents set out the procedures to be followed for computer-related projects and requests. Copies of these documents are available from the the IT Liaison Group members or from the System and Data Resource Team within the IT Group.

All IT related requests must be passed to the business area representatives on the IT Liaison Group committees for discussion at the next meeting.

All projects proposals must be accompanied by a Statement of User Requirements (SUR). Copies of guidelines on producing SUR's are available via the IT Liaison Group members.

2.2 Acquisition policies

The policy of the Authority regarding the acquisition of information technology products is to purchase hardware and software from a 'preferred supplier' whenever possible. Our preferred supplier is currently SystemHouse Limited.

The actual hardware and software purchased depends on the specific business needs. All purchases on I.T. related matters are organised via IT Liaison representatives and must follow the NRA Scheme of Delegation and Financial Memorandum. It is a responsibility of *managers* to ensure that these are followed.

3 SOFTWARE

3.1 Software support

The policy of Information Technology is to provide support via the Helpdesk for a standard range of microcomputer packages so that *users* are able to derive the maximum benefit from the use of computers. To provide an effective service and to make efficient use of available resources a limited number of standard packages are supported at a high level covering all major application areas, other software packages are supported on a best endeavours basis. The current standard supported packages are set out in the appendix of this document.

It is recommended that, whenever possible, standard packages are used, since this will provide the *user* with the greatest degree of support from Information Technology. All problems should be reported initially to the Helpdesk on Reading (0734) 535700, who will log the fault and will be able to advise on the action and progress taken.

When contacting the Helpdesk, *users* should suggest their priority to be assigned to solving the problem as follows:

1 Very Urgent	-	Major system, network or partial network failure affecting 50 or more users.
2 High Priority	-	User without alternative access locally or groups of users without service.
3 Priority	-	All service affecting faults.
4 Low Priority	-	Non service affecting faults, or users with alternative access locally.

The *user* priority/urgency will be added to the Helpdesk problem number and support group assigned to the call. For standard supported software the normal target response times are 1, 2, 4, and 8 hours respectively.

3.2 Copyright and licensing

Software packages are protected by UK copyright law (Copyright, Designs and Patents Act 1988). Before any copying of software confirmation that such copying will not be in breach of copyright law, or any agreement or licence, must be obtained from I.T. All staff are expected to comply with copyright law and any breach will be regarded as a disciplinary matter. An I.T. software and hardware inventory check may be conducted at any time. If found in breach of copyright law you and your manager are liable to be prosecuted.

All software will be installed by Information Technology staff or a person authorised by Information Technology. *Users* should therefore under no circumstances copy or move proprietary software from one computer to another. Users should also note the precautions against computer viruses (see section 4.7).

All original Micro computer packages and software licences and original media must be stored safely and retained by the nominated user or manager.

To avoid infringement of copyright Departments should periodically review their software usage and needs. *Managers* should:

- ensure there are no illegal copies of software in use or stored on hard disks within their areas of responsibility;
- request additional copies of software packages where increasing use justifies it, via the IT Liaison group.

The Helpdesk can now maintain a register of all original software packages issued to *users* and abstracts from this can be requested to help in an audit of departmental software.

3.3 Maintenance and upgrades

Software maintenance options on microcomputer packages will be taken up whenever they are available, since they offer easy access to future upgrades in addition to technical support. Upgrades of packaged software will be purchased whenever they can be justified. All software upgrading will be carried out by Information Technology or preferred suppliers authorised by IT.

With all upgrades, Information Technology will try to ensure compatibility with previous versions of the software.

4 OPERATIONAL ASPECTS

4.1 Installation

The installation of all microcomputer hardware and software will be arranged by Information Technology. This will ensure that:

- all installations comply with IT Installation Standards for ease of support and maintenance;
- all Health and Safety procedures are complied with;
- any hardware modifications (e.g. the installation of an additional memory board) are properly carried out;
- the necessary electrical connections are made (e.g. to a printer or modem);
- the operating system is properly installed;
- all application software operates satisfactorily and is correctly configured.

Users are NOT permitted to move hardware, this must be arranged via their respective IT Liaison Representative, as only insured personnel are authorised to move equipment. Thus we can ensure procedures are adhered to, maintain installation integrity, and enable IT to update their records for maintenance purposes.

The standard operating system for microcomputers in the region is MS-DOS, the most widely used release currently being version 3.3. However, new machines are supplied with MS-DOS version 5. In addition to the operating system, IBM's Fixed Disk Organiser, a screen menu front end was supplied with version 3.3, and the DOS 5 Shell menu is currently installed on all new microcomputers as the standard menu after start up.

Each *registered user* is responsible for safeguarding any media and manuals for software installed on their computer. These should be retained for use as primary reference and as additional proof of ownership.

4.2 Operation

All *users* of microcomputers should receive training in the use of their microcomputers. The IT Group can provide advice on the training required and refer the users to the Personnel Training Officer who will organise any agreed training with the preferred suppliers.

Each microcomputer will be allocated to a nominated user (the *'registered user'*) who will be responsible for ensuring that:

- the security procedures are adhered to (see over);

- the equipment is always safely operated;
- only trained personnel use the equipment;
- only software obtained using procedures defined above is used;
- any equipment movements are arranged via IT and reported to the Helpdesk.

The Helpdesk maintains an asset register of computer hardware allocated to the *registered users*. All permanent changes of *registered user* are to be authorised via the Helpdesk. This is a responsibility of *managers*.

4.3 Safety

After installation of the hardware, it is the responsibility of the *registered user* to ensure that appropriate safety precautions are taken. This includes ensuring that:

- all electrical connections are securely made;
- all cabling is in a satisfactory condition;
- the equipment receives adequate ventilation;
- any maintenance record tag is in date.

Blown fuses should not simply be replaced without first investigating the cause. If anyone suspects that any computer equipment is faulty, this should be reported at once to the Helpdesk, who will advise what action should be taken and, may arrange for an engineer to repair the fault.

4.4 Security - physical

Having become small, valuable and often portable, microcomputers are likely to get stolen. Staff should take all practicable steps to minimise the risks. This includes:

- challenging any stranger who is using a computer, or attempting to remove a piece of equipment or acting suspiciously.

Staff using portable microcomputer equipment or taking microcomputer equipment out of the office must:

- store equipment in locked cabinets when not in use;
- keep equipment hidden from view, e.g. not on a car seat;
- have no confidential data stored on the hard disk.

Microcomputers should be protected from possible overheating by ensuring they receive adequate ventilation - at least four inches of clear space all around the machine is advisable. Unless there is a specific reason otherwise, the equipment should be switched off at night.

In addition to the fire regulations applying to the Authority's premises, all microcomputer equipment *users* should be aware of the nearest location of fire-fighting equipment, the location of First Aid points, and the designated First Aider and Fire Officer. Suitable fire extinguishers for use with electrical fires are the BCF/Halon type 1211 (colour code green) for use with class B fires.

Microcomputers should be kept clean and free from dust and dirt, which could impair performance. In particular, food and drink should be kept well away from computer equipment and media. All calls reported to the Helpdesk as a result of food or drink spillages will be charged to the individual.

All microcomputers should have stickers on them, the NRA-TR Asset Tags. These must not be removed, as the asset numbers identify the particular piece of equipment.

Any electrical equipment maintenance record tag should be checked for being 'in date'. Equipment not in-date must not be used.

The Helpdesk must be informed immediately of any incident involving damage to or loss of computer equipment.

4.5 Security - media and backups

Microcomputers are vulnerable to losses of data. *Users* must implement their own routines for taking regular copies of data and programs held on their computer. Please refer to the 'PC Backup Procedures Guide' document, a copy of which is attached and more copies are available via the Helpdesk. The following should form the basis of establishing backup routines:

- backup tapes and disks should be clearly labelled to identify their contents and the date the backup was taken;
- backup procedures should be periodically tested to ensure that recovery of stored files is possible;
- backup tapes and disks should be kept in locked, fireproof and heat-proof cabinets, (where available);
- backups should be retained for a sufficient period;
- a backup set should be regularly stored off-site in a secure location, together with instructions for the recovery of information;
- the rate of change of data and the value of the data should be considered.

All magnetic storage media should be stored in a clean environment, safe from liquids, dust etc, and away from other magnetic fields, such as telephones. Floppy disks should always be kept in their protective sleeves when not being used.

The preferred software for backing up data on microcomputers is the DOS operating

system backup for floppy diskettes, and Everex or TapExchange for tape backups. One of these options should be available on all microcomputers with internal fixed disk storage devices. Where large amounts of data are involved a backup system using magnetic tapes should be used.

Instructions on the use of backup software and advice on designing backup schedules can be obtained from the Small Systems Team, IT Group, Reading (0734) 535851. For information on approved firesafes please contact the Facilities Computer Manager on Reading (0734) 535799.

4.6 Security - logical access control

Unauthorised access to data that might lead to the release of confidential information or the risk of corruption of data can be reduced by using passwords. Classified information must **never** be placed on the hard disc of a personal computer, (see Head Office security memorandum 'Security - OP/EM/002 PIGN' reference number RD113/KJN/E4/9/2).

There are two types of password:

Power up password - once set this will be required each time the computer is switched on. This is a very effective way of protecting data and programs. Managers are responsible for the safe storage of passwords so that authorised staff only have access. It is possible - although not easy - to gain access should a boot up password be lost or forgotten. This feature is not available on all existing PC's around the region.

Software password - this can be set for certain individual software packages, or sets of data within a package. Take care when such passwords are set. Often it is not possible to recover data should a software password be lost or forgotten. A secure record of such passwords should be kept. Software passwords may be registered with the Helpdesk.

The following advice on the use of password controlled systems should be followed:

- users must always logout of any network connection when leaving their desk;
- a password should have a minimum length of 5 characters;
- it should not be wholly numeric;
- it should be easily remembered but not easily discoverable. If a password is forgotten, the data could possibly be lost forever;
- it should be changed whenever you suspect it has become known to an unauthorised individual, and at regular intervals e.g. every 90 days;
- all written records of passwords must be kept securely;
- *users* are responsible for keeping other relevant personnel informed of

passwords and for keeping passwords securely;

- passwords for boot-up and access to packages also rely on equipment being switched off when not in use, or when staff are not in the room;
- passwords must be changed when staff transfer or leave.
- problems with passwords must be reported to the Helpdesk.

4.7 Security - viruses

A microcomputer virus is a programmed routine deliberately created, and usually added to a legitimate program, with the intention of interfering with the normal operation of a microcomputer resource, either for fun or maliciously. The main characteristics of viruses are as follows:

- they are hidden to avoid detection and removal;
- they are self-replicating to ensure the continued and contagious infection of computer resources;
- they interfere with normal operations in various ways - by deleting files, corrupting data, slowing the system as they use up resources, displaying messages and creating system and disk errors.

Viruses can be spread by performing any function on a microcomputer which causes an infected program to run. This includes starting up a microcomputer from an infected disk (hard or floppy), and running a program that contains virus code.

To protect the Authority's computers from the threat posed by viruses, the following rules should be followed:

- pass to Information Technology all floppy disks received from external sources so that they can be checked for viruses. This includes disks from other NRA regions and disks returning from external sources;
- remember to take regular clearly labelled backups to minimise damage in the event of a virus attack;
- never attempt to install software yourself, especially free software, e.g. games and demonstrations;
- all hiring of computer equipment should be done through Information Technology so that the appropriate precautions can be taken;
- never link your computer directly to a non-NRA computer.
- all micro computer links to any other computer must requested from and installed by the IT Group.

If any abnormalities occur in a computer's operation - including unusual screen effects - the equipment should be switched off and the I.T. Helpdesk notified immediately. The equipment should not be turned on again by *users*.

4.8 Good operational practice - file management

Good file management is a key element in ensuring that efficient use is made of computer resources. Each item of application software will be installed to IT Group Installation Standards in its own directory on the hard disk to keep it isolated from other applications. Furthermore application data is also held in a different directory to the programs. Within the data directories, *users* can create their own sub-directories for storing data files. *Only competent users* should attempt such operations. *Users* should also adopt an appropriate naming system for their data files so that their contents can be easily identified.

Each *registered user* should regularly review the contents of the hard disk, archive off - and then delete - any data files that are no longer required. This will:

- free up space on the hard disk;
- ease organisation of programs and data;
- reduce the time required for backups;
- make the system faster;
- ensure that *users* are following file naming conventions.

4.9 Software Support

Software support will be provided by Information Technology. Response times will be quicker and the quality of the support higher for standard software as detailed in Appendix 1, therefore standard packages should be requested and will be specified by the IT Group whenever possible.

The first point of contact for any problem relating to microcomputers is the I.T. Helpdesk, on Reading (0734) 535700.

4.10 Maintenance

Microcomputers used by this Region are covered by a maintenance contract with SystemHouse Limited. The response time under this contract is eight working hours, within which time SystemHouse will attempt to repair the equipment on-site. If repairs have to be carried out off-site and will take longer than two days, SystemHouse are contracted to lend a similar product for the duration, subject to availability.

All equipment faults should be reported to the Helpdesk who will:

- maintain a log of all reported faults;
- arrange for an engineer to repair the equipment, if necessary;
- monitor the response times under the maintenance contract to ensure

an efficient and cost-effective service is received.

- liaise with the problem resolution group and the user to ensure user awareness.

5 SYSTEMS DEVELOPMENT

5.1 Internal developments by Information Technology

Special business needs may result in application development performed on behalf of users. These projects are driven by the IT Liaison Groups via the National and Regional Information Systems Steering Groups, and managed and implemented by the Systems and Data Resource section of the IT Group.

5.2 Internal developments by users

Users contemplating developing a small application are encouraged to use the 'dBASE IV' software package and referred to the 'The Survival Guide to the Development of Database Applications' document, which details a structured approach to application development. Copies of this guide can be obtained from the Small Systems Team on Reading (0734) 535851.

6 DATA PROTECTION ACT 1984

6.1 Responsibilities of users

The Data Protection Act 1984 applies to personal data that are processed automatically. It gives individuals rights of access to personal data that is held by others. Individuals can apply to a court to have inaccurate data rectified or erased and can claim compensation for damage due to its inaccuracy, loss or unauthorised disclosure or access.

Data are defined as 'information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose'. The definition therefore includes data processed on microcomputers. The Act, however, carefully avoids using the word 'computer', as it is the use that is made of automatically processed data that is to be controlled, not just that processed on a particular type of equipment. Records kept entirely manually are excluded.

Personal data means data, as defined above, consisting of information relating to an individual who can be identified from the data itself or other information held. The Act does not regulate data held about deceased persons or legal persons (e.g. corporations).

Under the Act, personal data should be:

- obtained and processed fairly and lawfully;
- held only for specified and lawful purposes;
- protected against disclosure incompatible with those purposes;
- adequate, relevant and not excessive in relation to its purposes;
- accurate and up to date;
- kept for no longer than is necessary;
- available to individuals who shall be entitled at reasonable intervals and without undue delay or expense to be informed by the data user whether he holds personal data on that individual who should have access to, and copies of, any such data;
- subject to appropriate security measures against unauthorised access, alteration, disclosure or destruction, and against accidental loss or destruction.

The Authority is registered under the Act to hold personal data for certain specified purposes. Computer *users* should ensure that any proposed use is covered by the registration. Any questions regarding compliance should be directed to the Systems and Data Resource Manager on Reading (0734) 5761.

7 COMPUTER MISUSE ACT 1990

7.1 Introduction

This Act came into operation in August 1990 making it a criminal offence for anyone to access or modify computer-held data or software without authority or to attempt to do so. The Act creates specific offences to deal with the problems of hacking, viruses and unauthorised modification of software and data.

7.2 Responsibilities of users

The Act places no additional obligations on *bona fide* computer *users*. It does however introduce powers to prosecute those that deliberately and without authorization, misuse computer systems belonging to their employers or to third parties.

7.3 Consequences

Therefore those using computers without proper authority risk imprisonment as well as disciplinary action.

8 NETWORKS

The person primarily responsible for the smooth operation of a local area network is the nominated user or 'local network administrator', who is always a key network user. The main duties of the network administrator are to:

- control access to the data held on the file server, by ensuring passwords are kept secure and no unauthorised access is allowed;
- ensure the file server back up process operates correctly and that the tapes are cycled, clearly labelled, and securely stored;
- monitor the performance of the network;
- encourage regular 'housekeeping' on the data stored on the file server, asking users to archive and delete files not regularly used;
- inform the Helpdesk immediately of any problems.

8.1 Network Support

All maintenance and support work performed on the regions networks is provided by the IT Group. The network software supervision is provided by the Small Systems Team, the hardware and cabling maintenance is provided by Computer Facilities. Problems with the operation of a network must be passed to the Helpdesk who will inform, and chase, the relevant support group.

8.2 Network security risks

Failure to comply with the security and backup procedures (see section 4.5) have far greater consequences on a computer network, and therefore must be stringently adhered to.

8.3 Network software licensing

The rules on software copyright and licensing set out in section 3.2 apply as much to networked microcomputers as to individual machines. Therefore, software held on one microcomputer should not be copied via a network to another machine.

Many software packages for stand-alone microcomputers are also available in network versions, which can be held on the file server and accessed from any workstation on the network. The licence agreements of such software usually specify the *maximum number of users* of the package permitted at any one time. Care will need to be exercised to ensure that a licence allowing a sufficient number of *users* is purchased and that the maximum permissible under the licence is not exceeded.

8.4 Network connections to mini and mainframe computers

The security risks associated with PC networks also apply where microcomputers are networked to mini and mainframe computers. Misuse of equipment and software could have a serious impact. Transfer of viruses is a potential risk. All *user* area details - including passwords - should be kept securely, not programmed into function keys or held in script files.

9 TRAINING

Following the installation of a new microcomputer, the *user* can be offered advice by IT on appropriate training. Such training is organised on the user's behalf by the Personnel Training Officer with the preferred supplier.

Appendix 1

Supported software

Package	Application
MS-DOS ver 3.3 and 5	disk operating system
Lotus 123 rev 2.3	spreadsheet
Lotus 123 rev 3.1+	spreadsheet
Rapidfile	simple flat file database
Dbase III+ and IV	database
Lotus Freelance	graphical drawing
WordPerfect	word processing
DrawPerfect	graphical drawing
CA-Superproject	project management
CA-Supercalc	spreadsheet
Lotus Symphony	multi-function package incl. spreadsheet
DataEase	database
TapExchange	tape backup software
Everex	tape backup software
Relay Gold	communications and terminal emulation
PC-Link	terminal emulation
Novell Netware v2.X and 3.X	network operating system
Arcserve	network backup software

BACKUP PROCEDURES

FOR

COMPUTER SYSTEMS

WITHIN THE

NRA - THAMES REGION

Author: M. Michael (NRA-TR)
I. O'Hara (NRA-TR)

Date: 19th October 1992

Version: 2.00

Project: SP3331/44

CONTENTS

1. Introduction

Procedures and Issues

One of the most essential parts of any computing operation is the efficient and regular running of backups. Backups must be run for any computer system, from the simplest of PC applications to the largest of Mainframe systems. This section aims to point out the importance of backups, why they must be run, what needs to be backed up, and some of the simple rules of how to look after your backup media.

It is absolutely fundamental that as a PC user you take responsibility for backing up the system(s) you use, and the responsibility for that data, its security and integrity lies with you at all times.

1. **When** to Backup — Backups should be run at intervals which relate to the amount of usage your PC gets. For the majority of users this should be everyday. However, it is not always possible to ensure that this happens, but a backup should be made on a regular basis and **at least once a week.**

2. **Why** Backup ? — Information stored using any computer media may be subject to loss through accidental deletion, corruption, damage by computer virus, or by hardware failure.

   Backups, when made regularly and in an organised and well ordered fashion will allow you or the IT-Group to recover your data as soon as possible and with the minimum inconvenience.

3. **What** to Backup — It is not necessary to backup all your Hard Disk, as all of the application software disks should be available for installation in the case of hardware failure. What must be backed up is the information which you change or add to on a regular basis. This will include, for example, Wordperfect documents, spreadsheets and so on.

4. Where do I store my Backup ?

Your backup must be stored away from direct sunlight and magnetic sources. It is advisable to store backups away from the machine, perhaps in another building, in case of fire. Some users may have access to a fire safe which will protect the media from fire.

Floppy disks and tapes are known as removable storage as they are easily transportable. If your data is of a sensitive nature or if it is in danger of "disappearing" it should be kept under lock and key.

This document details the steps to be taken to perform a hard disk backup of the computer systems within the NRA-TR , both for standalone PC's and LAN's. This document does not provide the details for performing a hard disk restore because of the **destructive** nature of this process. Should you require to restore information to your system then you must contact the Help Desk in the first instance.

2. Methods and Media

It is important to have a logical approach to backups. Consider the effect of a Virus on a PC which only has one or two backups, one made a month ago and the other made several days previous:-

- o The most recent backup may contain the virus
- o The oldest backup may well contain practically no information which applies at the current time.

For this reason it is a good idea and good practice to use a cycle of backup media (disk or tape) of at least two weeks but preferably four weeks.

Example:

	Cycle 1	Cycle 2	Cycle 3	Cycle 4
Monday	1	6	11	16
Tuesday	2	7	12	17
Wednesday	3	8	13	18
Thursday	4	9	14	19
Friday	5	10	15	20

Contact I.T. if you are unsure which cycle to use for your requirement.

A method like this would facilitate the retrieval of the most recent information which did not contain the virus. This method would also allow a document, for example, to be retrieved which the user had not noticed had been deleted.

3. YOUR Responsibility

As a user you must take responsibility for YOUR DATA and for ensuring that a backup is performed regularly and in a proper manner.

Do not forget that backup media needs to be properly stored as it does become worn and will need replacing on a regular basis. The IT-Group are available to assist you in any issues regarding backing up and restoring data and also the type and formats of backup media best suited to your requirements. Make use of our services - IT'S FREE! -.

2.1 Floppy Disk Backup

The procedure described below is for backing up files from your Hard Disk PC to a floppy disk from the C:\ DOS prompt. The floppy drive can be either an A: or B: drive.

From the C:\ DOS prompt:

Type **CD** this will ensure that you are in the root directory.

Use one of the following command formats for backing up files from your C: drive to your floppy drive:-

BACKUP c:*.* A:

This command will backup all files in the root directory of C: to the A: drive.

BACKUP c:*.* A: /S

This command will backup all files in the root directory of C: and files in subdirectories of C:.

BACKUP c:\data*.* A: /F

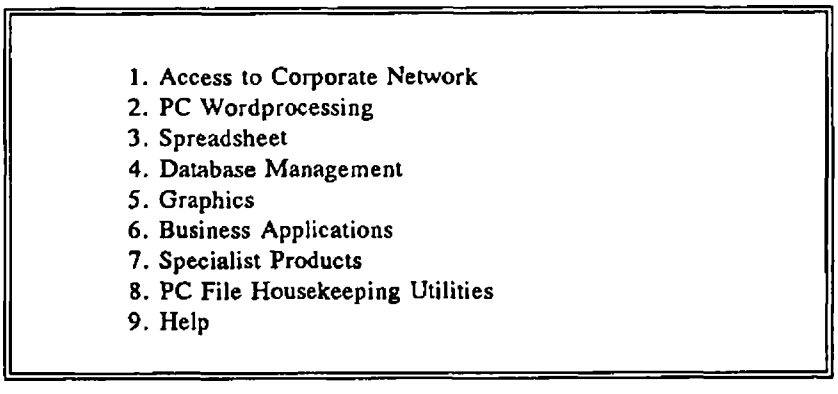
This command will backup all files in the \DATA subdirectory of the C: drive to the A: drive. The /F means that it will format the disk in drive A: if it is not already formatted.

See also the DOS **COPY** command in your system DOS Manual. (NOTE:- COPY will not link large files across multiple disks).

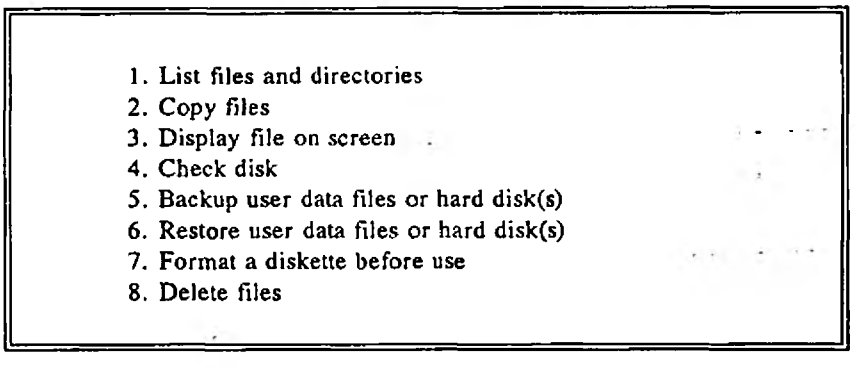
2.2 FDO Menu

The procedure described below is for backing up files from your Hard Disk PC to a floppy disk using the standard FDO menu system. The floppy drive can be either an A: or B: drive.

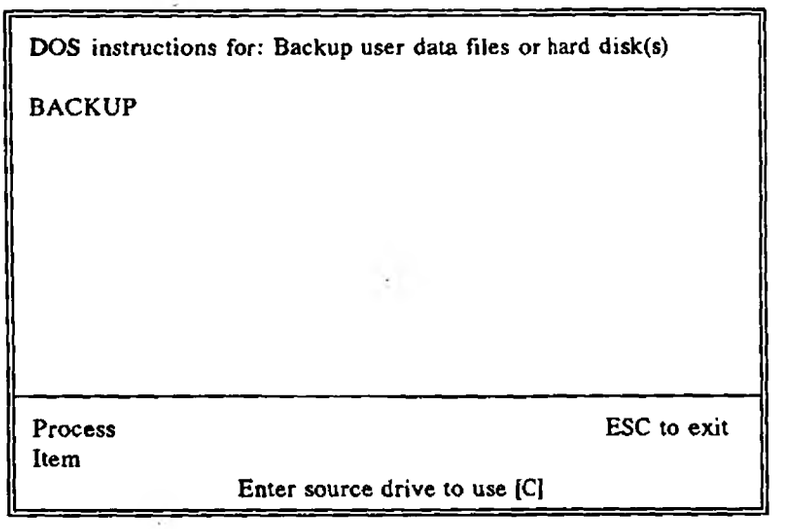
From the main menu:



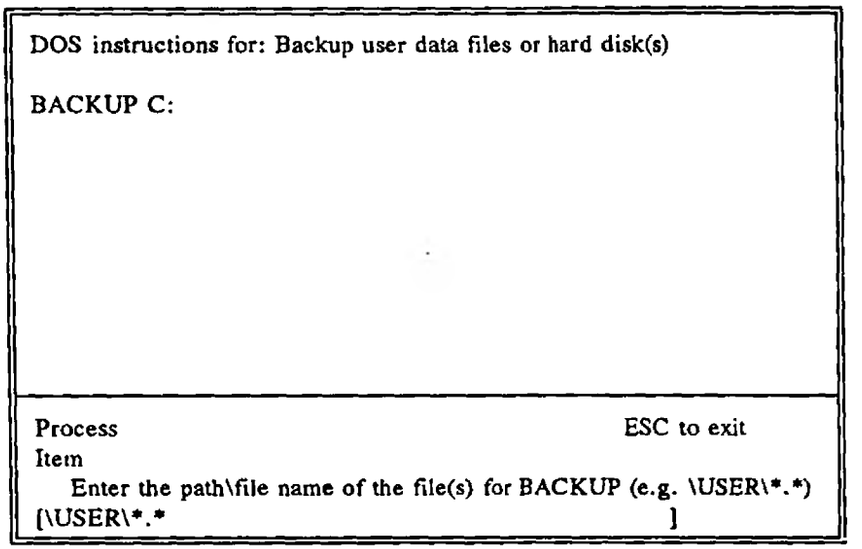
Select: **8. PC File Housekeeping Utilities.**



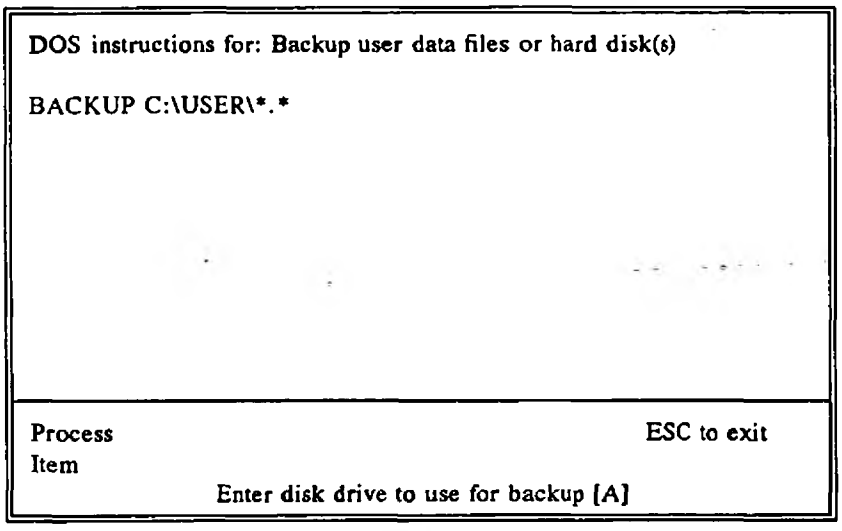
Select: **5. Backup user data files or hard disk(s).**



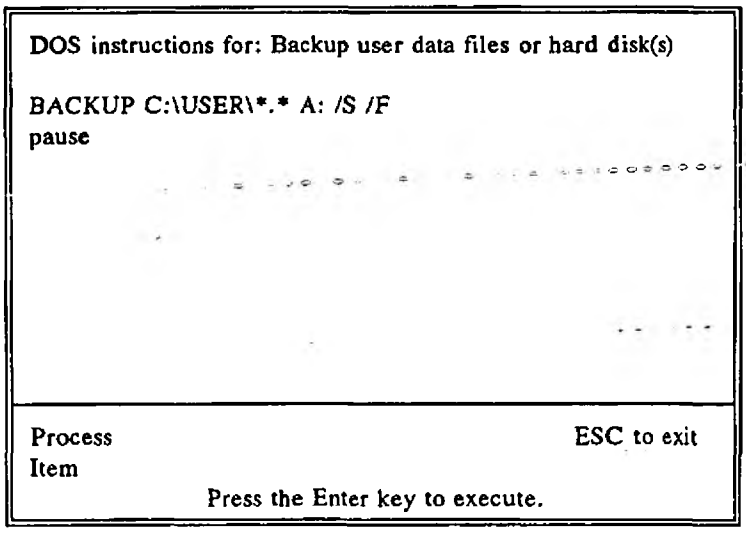
At this point, you will be prompted to enter the drive to be backed up. The default is the C drive. Enter the drive you wished backed up or press <RETURN> to accept the default drive.



Enter the path and file name of the files you wish backed up. The default is \USER*.* which you may change, or press <RETURN> to accept.



Enter the reference for the backup target drive. For floppy disk backup this will be either A (default) or the B drive (if present).



Having selected your target drive, the Backup command add the /S parameter to include backups of sub-directories, and also the /F parameter which will format the floppy disk if it is not already formatted.

2.2 FDO Menu

Pressing the Enter key will initiate the backup with the following message:-

Insert backup diskette 01 in drive A:

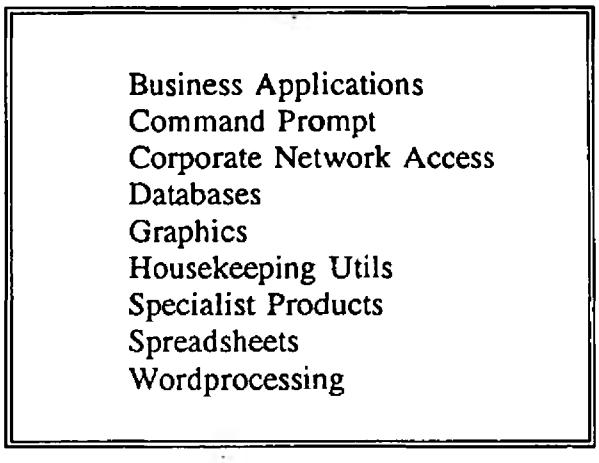
WARNING! Files in the target drive
A:\ root directory will be erased
Press any key to continue . . .

When complete the **PC File Housekeeping Utilities** menu will be represented.

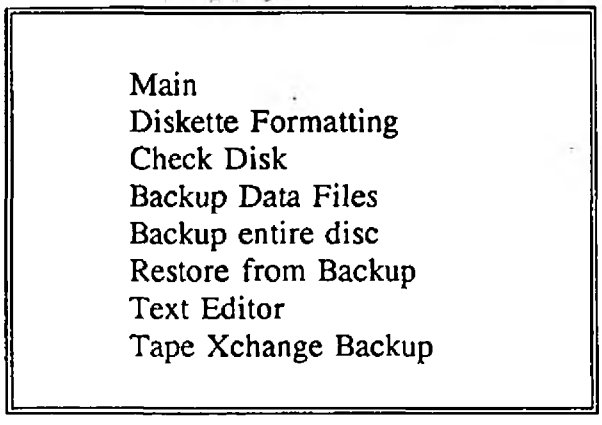
2.3 DOS 5.0 Shell Menu

The procedure described below is for backing up files from your Hard Disk PC to a floppy disk using the standard DOS 5.0 Shell menu system. The backup will only store files on drive A.

From the main menu:-



Select: **Housekeeping Utils**



Select: **Backup Data Files** to backup your data only in C:\USER, or

Select: **Backup entire disc** to backup the complete C: drive.

You will then be prompted with the following message:-

Insert backup diskette 01 in drive A:

WARNING! Files in the target drive
A:\ root directory will be erased
Press any key to continue . . .

Upon completion, the system will return you to the **Housekeeping Utils** menu.

2.4.4 Select Backup of all directories and files - Local Drives only using the arrow keys and ENTER.

2.4.5 Ensure that a tick is present against the items as listed above, if not select the item using the arrow keys and ENTER.

2.4.6 Press F10 to continue the backup.

You will then be presented with a message stating that the Software is identifying all available files.

When TapeXchange has located all available files a screen appears which allows you to include any special information you wish to include with the backup. Date and Time are included automatically.

The Session I.D. should be consistent with the type of cycle you are operating as outlined in the section on methods and media.

Comments can be included at your discretion.

2.4.7 Press F10 to continue.

Information is presented showing how much data has been selected, Tapes required, and the number of sessions already on the tape.

2.4.8 Press 'O' if you are using a new tape, to overwrite.

OR

2.4.9 Press 'A' to append the new session.

TapeXchange then gives a graphic display of how much of the backup has been completed and the files currently being archived. When the backup, and verification are complete press any key to return to the main menu.

2.4 TapeXchange 5.15

If you decide to do a selective backup (i.e. Backup Selected Directories and Files - Local Drives) TapeXchange will identify all available files and provide the following selection menu you for to select files you wish to include or exclude from the backup.

TapeXchange Backup Selection Utility - Version 5.15

Selected = Drives - 0, directorys - 0, files - 0, megabytes - 0.0000		
Active		
Drives	Directory tree	Files
C	\-| |--$DOS \| \|---DOS331 \| \|---DOS4 \| \|---GERMAN \| \|---NW286 \| \|---NW386 \| \|---OS2 \|--$TOOLS |--FDO	COMMAND COM CONFIG STN SD INI 16473 BAT FILE0002 CHK LOCALWPO MNU FSIZES QCV WORK LOG RAY BAT
1 Drives	132 directories	90 files
F10-Completed, ESC-Abort, T-Tag, C-Untag, F-Show/Hide files		

Navigate and select (the left and right arrow keys allow you to move between columns, and ENTER selects) :-

When your selection is completed, press the F10 key to continue.

The system then responds with: **'Looking for TapeXchange'**

A screen appears which allows you to include any special information you wish to include with the backup. Date and Time are included automatically.

The Session I.D. should be consistent with the type of cycle you are operating as outlined in the section on methods and media.

Comments can be included at your discretion.

2.4.10 Press F10 to continue.

Information is presented showing how much data has been selected, Tapes required, and the number of sessions already on the tape.

2.4.11 Press 'O' if you are using a new tape, to overwrite.

OR

2.4.12 Press 'A' to append the new session.

TapeXchange then gives a graphic display of how much of the backup has been completed and the files currently being archived. When the backup, and verification are complete press any key to return to the main menu.

You will then be required to complete Session information as explained in the previous section on conducting a full backup.

2.4.13 Upon completion, press any key to return to the main menu.

2.5 Everex Tape Streamer

The procedure described below is for backing up files from your PC to an Everex Tape Streamer.

2.5.1 Switch on your PC.

2.5.2 Switch on the Everex Tape Streamer and then insert a tape.

2.5.3 Select Everex Backup option from either your FDO menu or DOS 5.0 menu shell.

2.5.4 You will now be presented with the Everex Main Menus screen
Select **F5** for **Backup by File**.

2.5.5 You will then be prompted to **Specify file spec.** This tells the backup software which files are to be backed up and where they are located. Enter your backup options or press **<Return>** to accept the default shown on the screen.

2.5.6 Amend any subselections which are displayed and when you are satisfied that your selection criteria is correct, press **F8** to start the **BACKUP**.

2.5.7 If prompted, enter a tape number and tape label value, then F8 again.

2.5.8 Respond '**Y**' to proceed with the backup. The backup will then start.

2.5.9 **On completion** of the backup press **F2**.

2.5.10 **F10** to **EXIT.**

2.5.11 **<Return>** to confirm exit. The tape will then rewind.

2.5.12 When the tape has rewound, press F10 to exit, and then <Return> to go back to your FDO/DOS menu.

3.1 Mountain Series 2100 8mm 2.2Gb

The procedure described below is for backing up files from your LAN File Server PC to a tape using the Mountain Tape Streamer Series 2100.

3.1.1 Switch on the PC Workstation that the Tape Streamer is attached to or, if it is already switched on perform a soft reboot **<Ctrl-Alt+Del>**.

3.1.2 Press the **Button** on the Tape Streamer to open the device.

3.1.3 Insert a **Tape** with the red flag facing up.

3.1.4 Close the device to start **<Backup>** procedure.

3.1.5 At the **'Login'** prompt type **'BACKUP'**.

3.1.6 Followed by the password.

3.1.7 Type in the second Password to lock the keyboard from further use.

3.1.8 Switch off the monitor.

3.1.9 Next morning when the **<Backup>** is completed check the printer for the following output messages:-

THIS BACKUP SESSION STARTED ON day name, DD MM YYYY
SERVER xx_NOV_yy_99
SOME FILES HAVE BEEN SKIPPED ON THE DATA VOLUME
CHECK THE SKIPLIST.TXT FILE ON THE ROOT OF THE DATA VOLUME
SOME FILES HAVE BEEN SKIPPED ON THE APPS VOLUME
CHECK THE SKIPLIST.TXT ON THE ROOT OF THE APPS VOLUME
ALL FILES BACKED UP ON SYS VOLUME
SOME FILES HAVE BEEN SKIPPED ON THE DATABASE VOLUME
CHECK THE SKIPLIST.TXT FILE ON THE ROOT OF THE SYS VOLUME

3.1.10 Switch on the monitor, the following message should be displayed:-

Backup logged out
Time: 99:99:99

3.1.11 Type the **Password** to unlock the keyboard.

3.1.12 At the prompt type 'C:' <return>

3.1.13 Followed by '**TAPE**'

3.1.14 A menu will appear, cursor along to the **<DIRECTORY>** option and press **<RETURN>**.

3.1.15 Record the backup details in the Log Book (see.....)

3.1.16 Press the **Button** on the mountain to **<Eject Tape>**.

3.1.17 Press **<ESC>** key until you reach the DOS prompt.

3.1.18 Reboot the system.

3.2 Novell Server Backup / Compaq 1.3/2.0Gb DAT

User currently only have to insert a tape on a daily basis. The system automatically performs the backup late evening and on completion ejects the tape.

APPENDIX A.

Batch Files

```
@echo off

rem  RUNBACK.BAT
rem  D Gibbs            11/2/92

rem  Mods to change working directory to SYS:BACKLOG
rem  D Gibbs 9/4/92

rem  This file automatically runs the fileserver backup overnight.
rem  It is called by ES - the Autorun Event Scheduler.

rem  It requires AUTORUN by AUTOSOFT, a PC automation product.
rem  This runs Novell SBACKUP.NLM via RCONSOLE from a workstation.
rem  The user BACKUP is automatically logged in.

rem  The Start - used during debugging
:start

rem  Change to the LOGIN drive
f:

rem  Run the LOGIN procedure - this exits to DOS after running
rem  the login script
autorun login c:\backup\login.key

rem  Capture output to the default printer
call pdefault.bat

rem  Map the drive that contains RCONSOLE
map m:=sys:system
m:
CD\BACKLOG
REN *.ERR *.OLD
CD\SYSTEM
rem  Run SBACKUP via RCONSOLE
autorun rconsole c:\backup\rconsole.key
```

```
rem  Now print the error log file....
rem  Change to the right directory
m:
:end
cd\backlog
echo ********* Backup Log File ******** > > PRN
COPY M:\BACKLOG\*.ERR LPT1:

rem  Issue a formfeed to eject last sheet from printer
echo
 > > prn

:end

rem  Logout from server
rem logout

rem  Now perform a cold reboot
c:\reboot cold

rem  End of file label - use during debugging
```

APPENDIX B.

Backup Log Sheet

Date	Tape	Volume Name	Volume Size (Mb)	Initials