2.3 Data and Physical Security

As we have mentioned earlier, the data you create is valuable and very difficult to rebuild if lost. The last line of defense is certainly a well-maintained backup schedule, however, depending on that schedule, you may still lose a day or a week of data. Here you will find tips on PREVENTING data loss.

The physical equipment is also subject to damage, neglect and liberation.

2.3.1 Data, Software and Hardware Liberation

FASTFACTS *System Responsibility*

Personal Computing Rule of Thumb:

YOU are responsible for the integrity and security of your system, software, and data. Protect them.

- Lock your door at night to ensure that equipment, software and data are not liberated.
- Copy sensitive classified or unclassified data to diskette, delete it from your hard disk, and keep the diskettes under lock and key.
- NEVER use non-TEMPEST equipment for CLASSIFIED work, or place CLASSIFIED data on a disk which cannot be removed or locked away.
- Data falling into the CLASSIFIED category requires the greater physical protection afforded by TEMPEST. If you are in doubt about whether TEMPEST equipment is required, get guidance from ISS and MIT.
- If your software has a File Protection/Encryption feature, use it for your sensitive data. (WordPerfect, for example, has such a feature called LOCKED DOCUMENT FORMAT.)
- Anything you don't want to unwittingly share with someone else should be locked away, as you might your specially blended Continental Coffee or 100 year old Scotch, so that it will still be there when you want and need it. Software manuals are particularly attractive items, easily overlooked during moves.

Please refer to The Fine Print for further information about user responsibility and liability.