



Every organization using personal computers (PC's) needs a formal set of security procedures. Our basic suggestions for a Personal Computer Security Program follow. You may reword it, and add items to it, to suit your particular needs.

- Obtain employee cooperation - Accomplish this by implementing your program slowly. Advise employees of procedural changes well in advance. Explain why the tighter security is necessary, and how it will be of benefit to them. Use examples.
- Develop a communal sense of responsibility by encouraging employee participation in the development of the program. Ask for suggestions. The effectiveness of your security program will be in proportion to the base of its support.
- Limit physical access to PC's - Computers which contain sensitive information, or act as ports to mainframes require a secure environment. Fortify perimeter security. Secure the computer's case so that internal boards, hard disks, etc. cannot be removed. Have an authorized users list for each machine. Verify identity and work orders of repair persons.
- Password access - A password code should be an integral part of the system access procedure. Advise users to: change passwords frequently, and use quality passwords (My/DoG - is superior to MY/DOG - is superior to ROVER, for example). They must not to reveal, loan, or write passwords down. Some password programs automatically request users to change passwords on a regular basis.
- Never leave an active terminal. Always *log-off* a terminal when not in use.
- Report altered data to the Security or department manager. Early detection of a virus, or forced access, will mitigate losses.
- Report suspected physical tampering to the Security department. You work hard to compile information. Protect it.
- Remove sensitive data from the PC when not in use. Diskettes should be removed and securely stored. The PC should be turned *off* and *locked*. This will erase information left in most PC's RAM memory; check the manufacturer's manual to be certain.
- Memory typewriters should not be left with confidential information stored in them. Purge confidential data regularly.
- Memory media, such as floppy disks, are very susceptible to destruction via physical abuse and magnetism. They should be

*To get back up and running, get running and back up.*

backed up and stored in secure locations to prevent espionage or sabotage; one on premises, one off premises.

- Do not rely on copy commands. PC copy commands often move data by sectors, thus moving more than the specified file. Sensitive information may inadvertently be passed along this way.
- Do not rely on deletion commands. Usually the commands 'delete', 'erase', or 'remove' only open up an area of memory to be rewritten over in the future. Data remains intact until new information is entered. This data can still be read using one of the many "reconstruction" utility programs available. The *format* or *initialize* command will usually erase the entire disk.
- Erase diskettes before disposal or transfer to other use. One acceptable method is total degaussing (bulk demagnetizing), the other is the use of a data shredder program. If this isn't feasible, just destroy the disks and use fresh ones. Disks are inexpensive.
- Do not routinely connect PC's to networks. Make sure it is necessary first. Remote access to a PC can result in information loss, or data tampering. This can be prevented by not logging into the network unless necessary, and turning power off when the PC is not in use.
- Computers connected to phone lines need access protection. Use modems that have a call-back feature or employ high quality password protection. When transmitting sensitive files, use encryption. Do not leave computers attached to phone lines unless this type of use is required on a continuous basis.
- Do not use unsolicited or borrowed software. It may contain instructions or programs designed to capture, alter or obliterate the user's data (aka. viruses, worms, Trojan horses, etc.). Virus detection software and hardware are available at very reasonable prices.
- Back-up all data and programs on a regular basis. Store the back-up copy in a secure, and physically separate, location.
- Store floppy, removable hard drive, and optical disks in special data strong boxes, available for individual PC users. These specially made containers provide protection from fire generated heat, as well as the by-products of fires (steam and soot) - all very damaging elements. Their locks should not be relied upon for protection against espionage. Media storage areas for confidential information require high security locks.

