



Branch Dental Clinic

*Information Systems
Security*

User Guide

February 2002

1. Password Protection

Users must understand it is their responsibility to keep their password confidential and to use only the password assigned to them. The security provided by a password depends on the password being kept secret at all times. If a user shares his or her password with someone else, the user may be held responsible for the actions committed by the person using his or her password. If a user suspects password compromise, he or she should report it immediately to the clinic Information System Security Manager (CISSM). CISSM shall take appropriate steps to change the password immediately.

- (1) Passwords should not be taped to desks, walls, or equipment, and should not be kept in wallets or purses.
- (2) Each user should commit his or her password to memory and should destroy any hard copy.

2. Computer Security

Users should not allow any unauthorized person to have access to their computer and should not answer questions from unauthorized individuals regarding the type of information being processed.

All users should ensure physical and environmental security in their computer area. This means locking doors after hours, protecting equipment from water damage, refraining from eating and drinking near the terminal or computer, etc.

Encourage all users to challenge unauthorized staff and all strangers in their computer area.

Encourage all users to report malfunctions and security incidents to their command ISSM as soon as possible.

Computer Virus Threats

Computer viruses are a major concern throughout the Department of Defense because they can destroy or alter data in a computer system or can be used to gain unauthorized access to government computer systems. The following steps will minimize the chance of damage from a computer virus:

- (1) Do not load or use any software from an unknown floppy disk. Until you first scan for virus. Do use only approved software obtained through and loaded by the CISSM or the Management Information Department (MID).
- (2) Always keep your backups current.
- (3) If you suspect a virus, stop all processing, do not power down your system, and call the CISSM for assistance.

Fire Protection

Be sure that you know where the nearest fire extinguisher (CO2 or Halon) and fire alarm box are located and how to use these items. Usually you will smell wires or components burning long before there are any flames. Turn off and unplug equipment immediately. Never use water on an electrical fire.

Microcomputer And Terminal Security

Limit Access to Your Computer or Terminal. Know those who use it, service it, and repair it. Use power switch locking devices when available.

Label All Diskettes. Indicate the classification level of SENSITIVE UNCLASSIFIED of the data or application on the diskette. Do not process any CLASSIFIED information.

Avoid Leaving Privacy Act and Sensitive Data on the Computer Screen.

Protect such information displayed on your terminal or computer screen. Do Not Allow Storage Media Which Have Contained Privacy Act Or Sensitive Information To Leave Controlled Channels.

Do Not Use Borrowed Or Unsolicited Software. These may contain programs or instructions specifically designed to capture or alter your data or application. Use of this software also may be a violation of Federal copyright law. In addition, no software or floppy diskettes used on personal computer shall be allowed on command computers in accordance with instructions from CO, NMIMC January 1994.

Protect Computer Equipment From Environmental Hazard. Do not eat or drink near your equipment or anyone else. A surge protector shall be used on all computer equipment.

Make Frequent Backup Copies of All Your Data Files. In addition, stop and save your data often while working. An electrical power interruption can cause you to lose all information entered since your last save operation.

Protect your diskettes and tapes.

- (1) DO NOT expose disks to magnetic or magnetized objects. Data can be destroyed, scrambled or wiped out completely. A color TV, CRT, electric motor, or other devices, can destroy data integrity. Screwdrivers, paperclip, car keys, or any metal object may also be magnetized.
- (2) Protect your floppy disks at least as well as you would the data that they contain.

EXAMPLES OF BREACH OF SECURITY

1. Sharing of passwords or unauthorized use of passwords.
2. Leaving a computer unattended while processing sensitive information.
3. Accessing sensitive records without a "NEED TO KNOW".
4. Intentional input of invalid or inappropriate data.
5. Using hardware, software, or data for personal business.
6. Violation of copyright infringement laws by installing exceeding the legal license currently owned by this command.. This is against the U. S. Government copyright laws. You can be sure that software is legal if installed by the MID department or trained clinic representative.
7. Failure to comply with the rules for protecting and disposal of privacy act or other sensitive data.
8. Not logging off and powering down computers and locking doors when leaving the office each day.