CHAPTER 9. SECURITY

9-1. POLICIES AND RESPONSIBILITIES. The basic policy, guidelines and procedures described in the HUD ADP Security Policies Handbook (2400.10) and the HUD ADP Security Procedures Handbook (2400.11) apply to all computer systems including microcomputers and word processors which are used to manipulate data.

The responsibilities of the ADP Security Officers, program areas, Regional and Field Officers, and Administrative Officers as described in Handbook 2400.10 apply fully to Office Information Systems.

All managers of OIS should read 2400.10 to ensure compliance with policy.

9-2. SOFTWARE LICENSING AGREEMENTS. Software packages acquired by HUD are subject to licensing agreements which restrict the use of the software. The Department does not own the software, it merely licenses the right to use the product while ownership continues to reside with the copyright holder. Managers are responsible for familiarizing themselves with the licensing agreements and ensuring that all use of software is in compliance with these agreements. Microcomputer users must realize that violation of licensing agreements is both a breach of contract and a criminal offense. Moreover, both the Department and the individual employee may be liable.

Most licensing agreements indicate that each software package may be used only with respect to one machine, copies of program diskettes may be made only for backup purposes and for no other reason, and software manuals are also copyrighted products and thus may not be reproduced under any circumstances.

9-3. ABUSE OF SOFTWARE AND EQUIPMENT. Managers are responsible for ensuring that the office information equipment and software which they manage is used only for appropriate purposes. Managers are held responsible for the physical security of equipment, software, and data in their charge. Managers must also establish methods for monitoring the use of equipment and software, and for limiting access to equipment, software, and data. Any Departmental employee who becomes aware of any abuse of software and/or equipment, is responsible for immediately reporting the alleged abuse through his/her manager to the Departmental ADP Security Officer in IPS.

9-4 PHYSICAL SECURITY OF OFFICE INFORMATION SYSTEMS. Secure all HUD- owned or leased OIS equipment to prevent theft, misuse and abuse. Place any sensitive and/or critical storage media under lock and key when not in use.

Secure microcomputer and word processing equipment through use of a device approved by the General Services Administration (e.g., anchor pads or cables affixed to work stations) to prevent loss or theft.

Keep computer equipment which is not physically secured in a secured room or cabinet when not in use.

Facilities Operations Division in Headquarters is responsible for procuring and installing security devices. In the Region, the Regional Directors of Administrative Services/Administrative and Management Services Divisions are responsible for procuring and installing security devices in the appropriate Regions.

Facilities Operations Division in Headquarters, the Regional Directors, Administrative Services Division or Administrative and Management Services Division, and Field Office Managers and Chiefs or their designees shall authorize and control access to secured equipment when repair, maintenance, or movement is required.

Individual employees assigned portable equipment on personal charge are responsible for assuring that this equipment is kept in a secured room or cabinet when not in use.

Additional procedures to be followed are:

- Never leave OIS equipment in a room unattended. Lock the doors if no one is going to be in the room.
- Place all OIS equipment away from entrances, but place it where it is visible to normal office traffic.
- Position secretaries or receptionists near entrances so that visitors are cleared before entering work space.
- Position a staff member's work station so he/she can control who gains access to the microcomputer area.
- Limit the number of entrances into offices.
- In unlocked offices, secure government-owned equipment with pads or cables. Make sure peripheral equipment is secured.
- Place software in a safe, locking drawer or locking file cabinet. Do not secure software in unlocked desk drawer.
- Use a log to record who uses the equipment and time and date of use.
- Do not allow eating, drinking or smoking near the equipment. Keyboards, disk drives, diskettes and tape cassettes can be damaged and data or programs lost if any food, smoke or dust comes into contact with them.

9-5. OPERATIONAL SECURITY. Adherence to the following procedures will ensure a degree of operational security.

- o Determine criticality and sensitivity of each application system (see Handbook 2400.10 for definitions).
- o Place any storage media (i.e., diskettes, hard disk, cassettes) that contain sensitive or critical information classified as S3, C3, or C4 under lock and key during non-working hours. Do not leave these media unattended during working hours.
- o Assign and execute responsibility for access control, use, and updating of files.
- o Establish retention dates for data files, programs, and related files. Be sure that these conform to the HUD Records Management Requirements where applicable. (See Files Management Procedural Supplement 222.31 Supp-1; Records Disposition Management Handbook 2228.1 ; General Records Schedules, Handbook 2228.2; Records Disposition Management: HUD Records Schedules, Handbook 2225.6).
- o Use a password system for any application system classified C3, C4, S3 and S4. Systems classified S4 should be considered for use of an encryption package. (See Handbook 2400.10 for definitions).
- o Change passwords, where used, whenever a staff member leaves the organization and on periodic basis to prevent unauthorized access.
- o Maintain an inventory of and regularly check to account for all software.

9-6. BACKUP DATA FILES. All files and applications programs of sensitive and/or critical office information systems must have backup copies on other storage media. Always store backup copies separately from originals.

9-7. LOSS, THEFT, OR DAMAGE: Report the loss, theft or damage to any microcomputer or word processing equipment, as with other personal property, on HUD Form 27, Report of Survey, as required by HUD Handbook 2235.7, Chapter 7. As required, notify local law enforcement agencies of loss or theft.

9-8. PRIVACY ACT. The Privacy Act concerns systems of records about individuals from which information is retrieved by personal identifiers such as name or social security number. The Privacy Act:

- o Limits disclosure of personal information to authorized persons and agencies;

- Requires that information in records be accurate, relevant, timely, and complete; and

- Requires the establishment of appropriate administrative, technical and physical safeguards to insure the confidentiality and security of records.

Developers of systems falling under the Privacy Act requirements and their managers are responsible for responding to these requirements by:

- Establishing access criteria and providing access only to persons meeting the criteria.

- Ensuring that data on file is accurate, up-to-date, and serves a legitimate agency goal.

- Establishing procedures to protect information from unauthorized disclosure, modification or loss.