

DEFINITIONS

- A. "Password" means a user-assigned computer system access word unique to individual users that must be used with a "user-id" to gain access to a computer-managed database of information.
- B. "Security" means maintaining security of confidential, computer-stored information that includes protection from:
1. Intentional or inadvertent deletion of essential data.
 2. Intentional or inadvertent alteration of data.
 3. Intentional or inadvertent introduction of inaccurate data.
 4. Unauthorized access to and/or copying of data.
- C. "User-id" means an identification assigned by Central Office MIS user coordinator specific to one "AR" or "Administrative Responsibility" to control access to computer-stored information.

PROCEDURES

Regional administrators will develop any additional procedures necessary to implement this policy.

- A. The primary responsibility for safeguarding information lies with individual computer users. Secondary responsibility lies with the MIS coordinator in each region and office/RHC. Tertiary responsibility lies with the DDD-MIS user coordinator in Central Office.
1. Terminals with access to confidential client data will not be left unattended in a state which would allow unauthorized persons to view such data.
 2. Passwords will be changed by users every ninety (90) days or more often.
- B. Computer users will include system documentation of security measures required for maintenance of data base integrity and confidentiality of data as part of the systems design and analysis phase. Computer users will document disaster recovery procedures and file back-up requirements.

