

**AUTOMATED PERSONAL PROPERTY MANAGEMENT SYSTEM (APPMS)  
AUTOMATION SECURITY STANDARD OPERATING PROCEDURE**

1. **PURPOSE.** This Standard Operating Procedure (SOP) provides guidance for the protection and operation of the Automated Personal Property Management System (APPMS) classified as a sensitive but unclassified (SBU) Automated Information Systems (AIS).
2. **SCOPE.** This SOP applies to all Commanders Logistics Chiefs and Property Book Officers, who are authorized or required to maintain a property book. The Automated Personal Property Management System (APPMS) Version 6.0 is mandatory for use with no exceptions. APPMS is currently deployed at over 64 sites within the Corps of Engineers and adherence to local and regulatory security regulations is expected.
3. **REFERENCE:** AR 380-19, 27 February 98, Information Systems Security.

4. **POLICY.**

a. This SOP will be revised as needed, but at a minimum, it will be reviewed every three years by the Information Systems Security Officer (ISSO) for the APPMS System. This person is currently Janet Mathis, (202) 761-5270.

b. The security of APPMS information is the responsibility of all personnel accessing the system. APPMS is interfaced/integrated with a defense automated information system; therefore, passwords must be controlled and protected to prevent unauthorized access, modification, use, destruction, or denial of use of the records maintained in both systems.

c. Safeguards used to protect both the equipment on which the information is processed and the data itself consists of security management, software and hardware security, established procedures, communications security, personnel security, document controls, and physical and environmental security.

d. Employees should contact their local Security Office for guidance if necessary.

5. **GENERAL.**

a. Information Systems Security Office (ISSO) duties. The ISSO is the point of contact for all matters relating to automation (e.g., computer) security. Questions or problems will be directed to the ISSO. Please see you local Security and Law Enforcement Office for the identity of your local ISSO if unknown.

b. Terminal Area Security Officer (TASO) Duties. The ISSO will appoint a TASO's in writing to maintain security awareness of APPMS and its media. This person should reside in or near the office where APPMS is used and/or resides.

## 6. PROCEDURAL CONTROLS.

a. Use of government time, equipment, or material in connection with unofficial government business is in violation of Army regulations dealing with conflict of interest. Further, any such use of government resources for non-governmental use will not be condoned and should be reported to your local Security and Law Enforcement Office.

b. Any unauthorized or intentional changes to the APPMS configuration (to include changes to the software or hardware, interfaces, etc.) should be reported to your local Security Office. Any proposed or planned changes should be coordinated with the Information Management Office for determination of the security implications due to the change.

d. The original APPMS software and documentation will be protected to prevent intentional or unintentional loss or destruction.

## 7. PERSONNEL BRIEFING, CONTROLS, AND TRAINING.

a. All users of APPMS will at a minimum, initially read and annually review the appropriate security regulations (i.e., AR 380-19) and this SOP. Personnel operating APPMS equipment are expected to be knowledgeable of AR 380-19 and this SOP pertaining to APPMS. A security training and awareness program for the users of APPMS should be provided by your ISSO as appropriate.

b. The ISSO will ensure the employee(s) operating or maintaining APPMS have been briefed on the threats, vulnerabilities, and risks associated with APPMS and the area. If applicable, emergency and or disaster plans will be discussed.

c. Employees will be briefed on copyrighted software policy, use of unapproved software, and the need for frequent back-ups.

d. Employees will be instructed to report immediately to the ISSO the compromise of data, passwords, or operational procedures, which endanger the operation of APPMS.

e. APPMS media, document storage, handling, accountability, and destruction will be discussed as appropriate.

f. Accreditation documentation will be protected to the degree that its compromise could jeopardize the security of the program and negate measures that would be implemented for data protection. At a minimum, this document will be marked and controlled as FOR OFFICIAL USE ONLY correspondence.

8. APPMS SENSITIVE POSITIONS: Individuals operating APPMS will be subject to the guidelines in AR 380-19, para 2-17. The ISSO/TASO and fellow employees who

become aware of adverse information or unusual behavior of employees will advise the Logistics Management Chief and the Security Officer, so that appropriate actions may be taken.

9. DATA SENSITIVITY AND LABELING: Authorization and positive identification must be established prior to access or release of sensitive data/information to an individual or institution. SBU media and output will be marked, labeled, and stored IAW referenced regulation. Markings will reflect the sensitivity of the information, e.g., FOR OFFICIAL USE ONLY if required.

10. ACCESS CONTROLS: Physical access to the room containing APPMS media, documentation, documents and the computer equipment will be controlled by the ISSO and APPMS user(s). Appropriate controls will be implemented to restrict visitors' access to sensitive information. Personnel are responsible for ensuring visitors are cleared and have a need-to-know if information is accessed.

Use of foreign nationals in positions that have access to APPMS is discouraged; however, when other factors necessitate this practice, requirements of AR 380-19 paragraph 2-18, and AR 380-7, will be followed.

#### 11. SOFTWARE CONTROLS.

a. Each office should be running APPMS 6.0 to ensure that the system is year 2000 compliant.

b. The ISSO will ensure all APPMS software used is approved, documented, and that employees observe restrictions for duplication. Coordination with Information Management personnel will be done as needed.

c. Original copies (e.g., master copy) of software will be write-protected (if possible), loaded on the computer, and then secured to prevent unauthorized modification/theft.

d. Employees will not remove the software from the office without advanced approval of the ISSO.

d. Anti-viral software will be installed on the computer which APPMS resides and on those computers that are use APPMS.

e. Manipulation, modification, or compromise of software or data will be immediately reported to the ISSO.

f. Users of APPMS are responsible for maintaining their respective files, documents, and back-ups. Each Property Book Office should have a printout of the data in the APPMS database at least once a month in case of back-up system failure. A copy of the data will be backed up and printed at least once during December 28-31, 1999 to

ensure data will be available should systems fail. A copy of the data should be printed September 28-30, 1999 to ensure there are no problems into the next fiscal year.

g. In the event of a fire or other disaster, back-up copies of data should be stored in an area separate from the location where APPMS resides i.e. stand-alone workstation or LAN. The storage location should afford all necessary degrees of protection. Marking, labeling, and storage requirements are the same for back-ups of data files stored on removable media.

12. **HARDWARE CONTROLS:** See Clearing, Purging, and Destroying of AIS or Media and Access Controls.

13. **PASSWORD CONTROL.**

a. Passwords will be used to restrict access to APPMS. Knowledge of individual passwords will be limited to the employee the systems administrator and the ISSO. Employees will obtain their passwords from their UPASS POC and be briefed on the classification, exclusiveness, prohibition of sharing password with other personnel, and about not writing the password down so unauthorized personnel might gain access.

b. Employees are required to inform the ISSO immediately if passwords are compromised, misused, or other potentially dangerous practices.

c. Passwords must not use common names or be easily guessed words, and must be alpha-numeric.

d. Passwords will be handled and stored at the level of the most sensitive data contained in APPMS FOR OFFICIAL USE ONLY.

e. Passwords will be changed every six months. By the systems administrator IAW AR 380 19, paragraph 2-15, they will be issued only once and will be retired when the time limit has expired, the user has been transferred to another duty, reassigned, retired, or discharged. If applicable, user-ids and passwords will be deleted as needed by the ISSO, System Administrator, or appropriate ISSO at the host level.

14. **AUDIT TRAILS OR MANUAL LOGS.** APPMS a multi-user system and must have an audit trail capability sufficient to reconstruct events should a compromise or malfunction occur. The Property Book Master Listing Report should be run weekly and given to the Property Book Officer for safekeeping. We caution each user to run this report the last week of December, 1999 to ensure all information is up to date in case of year 2000 system failure. A copy of the data should be printed September 28-30, 1999 to ensure there are no problems into the next fiscal year. In addition to the data, a roster of personnel names, user IDs, permission levels, and their passwords should be maintained by the ISSO and/or Property Book Officer.

15. **CLEARING, PURGING, DECLASSIFYING, AND DESTROYING OF AIS OR**

**MEDIA:** The ISSO will verify the procedure(s) used as adequate to preclude unauthorized access to AIS or media when no longer needed.

16. **MAINTENANCE:** Employees will report APPMS problems to the APPMS Hot Line at: 202-761-4516, if they cannot be resolved locally. The Local Information Management Office is responsible for correcting site specific software and hardware problems.

17. **CONTINUITY OF OPERATIONS PLAN (COOP).**

a. This COOP applies to APPMS data and software.

b. APPMS users are responsible for routinely backing up their files and properly marking, controlling, and storing them on appropriate removable media or hard disks (if any). Original copies of operating and application software will be write-protected (when possible) and properly stored.

c. In the event of a fire or other disaster, original copies of software and back-ups should be stored in an area separate from the APPMS. The storage location should afford all necessary degrees of protection. Access controls in place and the sensitivity of the information will be considered for alternate storage locations.

d. Communications must be considered when choosing an alternate location in the event of an emergency. As a minimum, the alternate location must have access to a high speed modem and a phone line to continue operations with the CEFMS program. In the event communications cannot be established immediately with CEFMS property will be manually added to the APPMS system and hand receipted to users. The remarks section of APPMS will be annotated "ADDED TO APPMS WITHOUT CEFMS PROCESSING" which will provide a means of correcting integrated system problems when communications are reestablished with CEFMS.

18. **CLASSIFIED PROCESSING OF DATA IS NOT PERMITTED.**