

9. SYSTEM SECURITY

9.1 Mode of Operation

In accordance with (IAW) DOD Instruction 5200.40 and AR 380-19. The system sensitivity designation will be unclassified-sensitive (US2). Mode of operation and accreditation utilizing the generic plan will be submitted by the host-site (Fort Lee).

9.2 Security Responsibilities

- Information System Security Officer (ISSO).

An ISSO will be appointed for each AIS. The following is a list of duties to be performed by the ISSO:

- Ensure systems are operated and maintained IAW DOD Instruction 5200.40 and AR 380-19.
- Ensure users have the required personnel security clearance, authorization, and the need-to-know. Include all users, operators, and managers associated with the system in all security training and awareness programs.
- Conduct threat and vulnerability assessments to enable the commander or management to properly assess risks and determine effective measures to manage such risks.
- Prepare, distribute and maintain plans, guidance instructions, and SOP concerning the security of system operations.
- Immediately report to the facility manager and Installation System Security Manager (ISSM) any attempts to gain unauthorized access to information or suspected defect that could lead to unauthorized information disclosure.
- Prepare or oversee the preparation of the site accreditation documentation.
- Establish a system for issuing, protecting, and changing system passwords.
- Ensure a Terminal Area Security Officer (TASO) is appointed for each terminal not under the direct control of ISSO and assures that TASO performs the duties listed below:

- Terminal Area Security Officer.

The TASO will perform the following duties, as required by the ISSO:

- Issue written instructions specifying terminal security requirements and operating procedures.
- Establish each terminal user identity, need-to-know, level of clearance, and access authorization commensurates with the data available from that terminal.
- Establish procedures to restrict entry of unauthorized transaction data.
- Monitor local compliance with security procedures.
- Assist the host system, ISSO, provide system security.
- Report actual or suspected security violations or incidents to the host-installation ISSO.

9.3 Software Security

Safeguards will be implemented into the AFMIS software to protect against compromise, subversion, or unauthorized manipulation as described below:

- Software that has been specifically developed or approved for use, or has been purchased or leased by an authorized U.S. Government representative will be used with any Army AIS.
- Valid documentation will support software used by programming, operations, and user personnel. Only personnel performing official duties should be allowed access to this documentation.
- Upon acceptance for operational use software must be kept under close and continuous configuration management controls to ensure that unauthorized changes are not made. A master copy of the software must be safeguarded and never used for actual production operations. Production copies of software should be generated from the master copy, as required. System and application program libraries will be protected and back-up copies maintained.
- Operational software may be modified and maintained only under rigorously controlled conditions requiring verification.

9.4 Hardware Security

Maintenance personnel should be observed during their maintenance operations by individuals with technical expertise to detect obvious unauthorized modifications.

9.5 Physical Security

AIS not having classified files on non-removable media should be kept in a locked office or building during non-duty hours, or otherwise, secured to prevent loss or damage. Users will log-off the computer when leaving the area.

9.6 Procedural Security

- These mechanisms are often most cost-effective and efficient methods of achieving these minimum security requirements. The ISSO oversees generation, issuance, and control of all passwords. Users will not have any control over choosing their passwords, unless such a choice is from one or more randomly generated by the system. The TASO may assist in issuing passwords in his or her respective area. All passwords must be generated and installed on the system by the ISSO, ISSO-approved assistants, or ISSO-approved software.
- AR 380-19 paragraph 4-11 provides a banner that will be included as part of the log-on screen on all computer systems.
- Security on Windows NT 4.0 and Mintronix Dynova P5000 POS.

To successfully meet account requirements, account policies should be configured to correspond with the following:

Windows NT 4.0 Account Policies:

Maximum Password Age	Less than or Equal 180 days
Minimum Password Age	Greater than or Equal to 1 day
Minimum Password Length	Greater than or Equal to 8
Number of Passwords stored in history	Greater than or Equal to 24
Account Lockout	Enabled
Lockout Duration	Forever
Bad Logon Attempts	Less Than or Equal to 3 attempts

To successfully meet audit requirements, audit policies should be configure to

correspond with the following:

Windows NT 4.0 Audit Policies

Logon and Logoff	Success and Failure
File and Object Access	Success and Failure
Use of User Rights	Success and Failure
User and Group Management	Success and Failure
Security Policy Changes	Success and Failure
Restart and System Shutdown	Success and Failure

To successfully meet the user requirements, user policies should be configured to correspond with the following:

Windows NT 4.0 Users

Administrator Account	Renamed
Guest Account	Renamed
Guest Account	Disable
Password Requirements	All Accounts
Password Expiration	All Accounts
Dormant Accounts	Disable after Thirty Days

To successfully meet security requirements the following Service Packs, Patches, virus protection software and Hotfixes will need to be installed:

Windows NT 4.0 Service Pack Installations

Microsoft Windows NT 4.0	Service Pack 6A
Microsoft Windows NT 4.0	C2 Hotfix

- Security on UNIX Base Operating Systems.

Unix based hosts need to meet the minimum required setting relating to account policies.

Maximum Password Age *	Less than or Equal 180 days
Minimum Password Age *	Greater than or Equal to 1 day
Minimum Password Length	Greater than or Equal to 8
Number of Passwords stored in history	Greater than or Equal to 24
Account Lockout	Enabled
Lockout Duration	99999
Bad Login Attempts	Less Than or Equal to 3 Attempts
Guest Accounts	Disable
Passwords Requirement	All Accounts
Passwords Expiration	All Accounts
Dormant Accounts	Disable After 90 Days

Note: * Indicates parameters can be changed using the SCOADMIN tool selecting the “ Account Manager “ option.

- UNIX Operating Systems Ports and Services.

Any existing and all future operating system installations must be carefully audited and any non-essential ports and services must be disabled. At a minimum the following should be considered:

DISABLE UNDER ALL CIRCUMSTANCES	STRONGLY ENCOURAGED TO DISABLE	DISABLE WHEN NOT REQUIRED FOR NORMAL OPERATION
Echo, daytime, chargen, finger, discard, qotd, bootp, gopher, news	Unix rcommands (rlogin, rexec, etc), replace telnet with ssh	Unused services