



DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY GARRISON
U.S. ARMY SIGNAL CENTER AND FORT GORDON
FORT GORDON, GEORGIA 30905-5000

REPLY TO
ATTENTION OF:

IMSE-GOR-HRM-C

OCT 13 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Electronic Military Personnel Office (eMILPO) MEMORANDUM
Number 5 – Terminal Access and Area Security

1. This memorandum supersedes eMILPO Memorandum Number 5, subject as above, dated 14 Mar 08.
2. References:
 - a. AR 380-5, Department of the Army Information Security Program, 29 Sept 00.
 - b. eMILPO Functional Guidance, 14 Sept 06.
 - c. Soldier Record Data Center – functional proponent Army Human Resources Command.
3. The purpose of this memorandum is to establish procedures and guidelines for controlling access and area security for eMILPO workstations. A summary of responsibilities for the Terminal Area Security Officers and operators is at Enclosure 1.
4. Each individual permitted access to eMILPO will be given a Security Briefing. An example of this briefing is at Enclosure 2.
5. Please be advised that it is the Work Center Supervisor's responsibility to notify the Personnel Automation Branch System Administrator once an eMILPO user departs or is no longer authorized access so the account can be disabled.
6. This memorandum will be maintained on file by each Fort Gordon unit/activity.

- 2 Enclosures
1. Terminal Access and Area Security
 2. eMILPO Personnel Security Briefing


JOHN MCINTYRE
Director of Human Resources/
Adjutant General

DISTRIBUTION:
Project Manager, AKIMA
(CONT)

IMSE-GOR-HRM-C

SUBJECT: Electronic Military Personnel Office (eMILPO) MEMORANDUM
Number 5 – Terminal Access and Area Security

DISTRIBUTION: (CONT)

POB

PSB

Str Mgt Br

Transition Point

TSPB

Cdr, U.S. Army Garrison

Cdr, 116th MI Gp

Cdr, 442d Sig Bn

Cdr, 15th Sig Bde

Cdr, 73d Ord Bn

Cdr, 35th Sig Bde

Cdr, 67th Sig Bn

Cdr, 513th MI Bde

Cdr, 297th MI Bn

Cdr, 35th MP Det

Cdr, EAMC

ADL

DENTAC

Cmdt, NCO Academy

Cdr, 3d Region

Cdr, 249th Med Hosp

Cdr, 206th MI Bn

Cdr, 369th Sig Bn

Cdr, 447th Sig Bn

Cdr, 551st Sig Bn

Cdr, 63d Sig Bn

Cdr, 56th Signal

Cdr, 202nd MI Bn

Cdr, 56th SC HQs

Cdr, 7th Signal Command

TERMINAL ACCESS AND AREA SECURITY

1. The Information Management Officer from the Office of the Deputy Chief of Staff for Personnel has designated eMILPO data as Unclassified-Sensitive 2 (US2). This designation identifies unclassified information, which must be protected to ensure its availability or integrity. This information may also require protection from foreign intelligence services or other unauthorized personnel to ensure confidentiality. In order to protect the US2 data, eMILPO implements the Controlled Access Protection requirements, Class C2. The Class C2 protection enforces discretionary access control by making users individually accountable for their actions through login procedures, auditing or security-relevant events, and resource isolation. The eMILPO requires protection to ensure confidentiality, integrity of data, and a high degree of availability.

2. Security Roles and Responsibility. Everyone accessing eMILPO is responsible for maintaining security of the system. However, the Information Assurance Security Officer (IASO), System Administrator (SA), and Work Center Supervisor (WCS) have a greater degree of responsibility. An IASO, SA, and WCS must have the clearance for all information residing on the system. The eMILPO relies on additional accountability, a special environment, and physical security to ensure that only authorized personnel can operate as an IASO, SA, and WCS.

a. System Administrator. The SA is responsible for maintaining the system security in coordination with the IASO. The SA assigns accounts based on Army Knowledge Online (AKO) userids and passwords. The SA has the capability to add new users, change user access permissions, and retire user accounts.

b. Information Assurance Security Officer. The IASO is responsible for the overall security management of the eMILPO system. The IASO is to be notified of all security incidents; and participates in the investigation and resolution of the incident.

c. Information Security. Measures and controls must be in place to protect an automated information system against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of data. Countermeasures include:

(1) The use of AKO userids and passwords for the identification and authentication of all eMILPO users.

(2) Periodically checking the audit log, the system user log, and limiting users to the information needed to perform their mission.

(3) Ensuring that all information processed by eMILPO is protected, accurate and available only to those who need the information in a timely manner.

d. Physical Security. The application of physical and control procedures as prevention against threats or attacks to resources and sensitive information. A few general guidelines for physical security are:

- (1) Physically protect hardware and media.
- (2) Logoff the system or use password enabled screen savers when operators temporarily leave the area of the workcenters.
- (3) Keep areas around the workstation organized.
- (4) Be aware of the locations of physical communications lines and protect the lines from unauthorized access.

eMILPO Personnel Security Briefing

eMILPO User Responsibilities:

System security requires protection against unauthorized disclosure, modification, and destruction of computer systems data, input/output, and all processing. It is the user's responsibility to ensure continuous protection of the operating system and all data files. Only a user with a valid userid and password may access the system. The System Administrator (SA) grants users access privileges to the eMILPO application. The Trusted Computer Base (TCB) requires the user to identify him/herself to the system before beginning to perform any other actions. An owner or proponent will be identified for each file or data grouping on the Automated Information System throughout its life cycle.

All users are required to comply with the following:

Safeguard assigned, unique password. Passwords must never be written down or otherwise stored in readable form; users are prohibited against disclosure of passwords to other personnel.

Report changes of personnel status (e.g., emergency leave, or any unusual personnel situations) to the SA or Work Center Supervisor (WCS).

Report any suspected security violations (e.g., observing other users exchanging passwords, or passwords being written down, etc.) to the SA, WCS, or the Information Assurance Security Officer.

As a user/operator, the system will be operated in accordance with the site Standard Operating Procedure, applicable regulations, manuals, and directives. The TCB will enforce individual accountability by providing the capability to uniquely identify each individual Automated Data Processing system user.

Report system problems or anomalies immediately to your SA. For example, if a user is denied access to normally assigned functions, or has the ability to gain access to functions not normally associated with one's duties, these are problems that must be reported in order to determine cause and effect.

Signature: _____ Date: _____

Printed Name: _____

Brief Type: Initial: _____ Date: _____ Annual: _____ Date: _____