



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT AGENCY
SOUTHWEST REGION
1204 STANLEY ROAD, SUITE 9
FORT SAM HOUSTON, TX 78234-5009



SFIM-SW-PL-I

12 DEC 03

MEMORANDUM FOR All Southwest Region Office (SWRO) Installation Management Agency (IMA) Personnel

SUBJECT: SWRO Policy Memorandum #7 - User Information Assurance (IA) Awareness Training

1. REFERENCES:

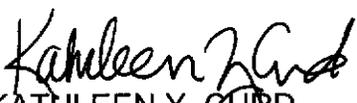
- a. AR 25-1, Army Information Management, 31 May 2002
- b. AR 25-2, Information Assurance, 14 November 2003
- c. Fort Sam Houston Installation Information Management Policy 25-02, Compromised Computer Systems, 26 November 2002

2. PURPOSE: To provide an understanding of IA awareness measures, procedures, and DA mandated user awareness certification training.

3. APPLICABILITY: This policy applies to all personnel assigned to SWRO, both Government (civilian/military) and Contracted personnel.

4. PROCEDURES: All personnel must receive IA awareness, computer user security training provided by the U.S. Army School of Information Technology, Ft Gordon, GA, located at G:\IMASWR\Computer Security Trng for User\Information Assurance\Index.htm. Current password-holders need an annual refresher briefing, and new users will receive the training before issuance of a password for network access. Upon completion, print and sign the "Information Assurance User Initial and Annual Refresher Training Brief" and send to Mrs. Chin Nittinger, Information Assurance Manager (IAM), SWRO.

5. PROPONENT: Plans Division is the proponent for this Policy Memorandum. POC is Mrs. Chin S. Nittinger IAM, SWRO at 221-9713 or Chin.Nittinger@samhouston.army.mil.


KATHLEEN Y. CURD
Chief of Staff

**Information Assurance
User Initial and Annual Refresher Training Brief**

Reference AR 25-2.

- 1. You are involved in a war over control of information. The outcome will determine if you or the enemy will have access to your information.** There are numerous information systems on Fort Sam Houston (FSH). These systems are vulnerable to computer hackers, Foreign Intelligence Services (FIS), terrorist, criminals, disgruntled individuals or groups.

- 2. Intruders have devised numerous techniques for breaking into our systems.** Once intruders gain entry, they appear as trusted members. The James Bond and Al Capone of today will use a computer to steal, modify or alter information.

- 3. As a user you are the first level of security and are responsible for:**
 - a. Protecting your password** - do not let others use your password. The intruder will use your password to quickly and easily by-pass most security measures. Your password must be "STRONG" (8 or more characters in length, combination of upper case, lower case, numbers and symbols), and be changed at a minimum every six months.
 - b. Controlling access to your PC** - do not let others have unsupervised access to your PC. They can gain entry to the network appearing as you and use your permissions and trust relations.
 - c. Check all disks for viruses' prior to use.** Preformatted disks are often contaminated. Do not download a file onto your PC without checking for viruses.
 - d. Knowing to report suspected intrusions, viruses and operating anomalies and reporting these incidents when they occur.** Report incidents to ITBC, ATTN: SECURITY DIV., Tel # 221-6580/8639.
 - e. Controlling network workload** - do not forward chain email, including virus warnings. The Fort Sam Houston DOIM will disseminate virus alerts and threat advisories. Report all chain e-mail or warnings to ITBC, ATTN: SECURITY DIV., Tel # 221-6580/8639, ITBC Security who will advise you of necessary action required
 - f. Ensuring Internet web browsers are configured and used in the most secure manner.** Your government computer is provided for official business. Personal use or use of programs that automatically provide private interest (sports, stocks etc.) updates consumes network resources and hamper the conduct of official business.

- 4. Safeguarding classified information** - do not process, store or transmit classified information on non-secure telecommunications systems. Official telecommunications systems, including telephones, facsimile machines, computer networks, and modems, are subject to monitoring for telecommunications security purposes at all times. **Use of official DOD telecommunications systems constitutes consent to telecommunications monitoring.**

- 5. ACKNOWLEDGMENT:** I acknowledge with my signature that I have read and understand the Information Systems Security guidance/policy above. If I refuse to sign this statement I will not receive a User-ID and password or be granted authorization to operate information systems. I also acknowledge receipt of my User-ID and password.

USER: _____
(Printed name)

DATE: _____

USER: _____
(Signature rank/grade)

**Information Assurance
User Initial and Annual Refresher Training Brief**

ANNUAL REFRESHER TRAINING:

SIGNATURE: _____ DATE: _____

SIGNATURE: _____ DATE: _____

SIGNATURE: _____ DATE: _____