

Fort Hood Pamphlet 25-25
23 October 2007

**Computer
User
Guide**



DEPARTMENT OF THE ARMY
HEADQUARTERS, III CORPS AND FORT HOOD
FORT HOOD, TEXAS 76544-5016
23 October 2007

*III CORPS & FH PAM 25-25

Information Management
COMPUTER USER GUIDE

History. This revision is an administrative revision. This is the second revision of this pamphlet.

Summary. This pamphlet is a guide to using information technology in the workplace. In support of information assurance, this guide prescribes procedures for using government computers (GCs) in a way that protects them against hackers.

Applicability. This pamphlet applies to military, Department of Defense (DOD) civilians, and DOD civilian contractor employees operating a GC

on the Fort Hood unclassified and/or classified LandWarNet (NIPRNet/SIPRNet).

Supplementation. Local supplementation of this pamphlet is prohibited without approval by the Directorate of Information Management (DOIM).

Suggested Improvements. DOIM is the proponent of this pamphlet. Send comments and suggested improvements to the DOIM, ATTN: IMWE-HOD-IM, Fort Hood, Texas 76544.

FOR THE COMMANDER:

JOSEPH L. ANDERSON
BG, GS
Chief of Staff

Official:



CHARLES E. GREEN, SR
Director, Human Resources

DISTRIBUTION:
IAW FH FORM 1853, S

Contents

1. Purpose, *page 4*
2. References *page 4*
3. Abbreviations and terms, *page 4*
4. Summary of change, *page 4*

*This pamphlet supersedes III Corps and Fort Hood Pamphlet 15 Oct 2001.

5. Your government computer (GC), *page 5*
6. What is the threat, *page 5*
7. How to obtain a government user account, *page 6*
8. Using your government computer (GC), *page 6*
9. Reporting computer security incidents, *page 11*
10. How to treat a government computer, *page 12*
11. Computer User Test, *page 12*
12. Conclusion, *page 12*

Appendix

- A. References, *page 14*

Glossary, *page 15*

1. Purpose

a. As a user of government furnished equipment (GFE), you can greatly affect the security of our networks. Protecting the information on those networks is called information assurance (IA). This guide is your driver's manual for the information highway and will help you do the right thing by showing you how to recognize and avoid the hazards awaiting you.

b. Before you can be issued a license to "drive," you must meet the minimum personnel security standards as outlined in Army Regulation (AR) 380-67 (The Department of the Army Personnel Security Program), paragraph 3-401, and AR 25-2 (Information Assurance), paragraph 4-14. You must take the Fort Hood (FH) Computer User Test and sign the FH Form 25-X33 (Computer User Agreement). This agreement is a promise to use Fort Hood's network responsibly and follow command policy on computer use. This guide tells you everything you need to know to pass the test.

2. References

Appendix A lists required and related references.

3. Abbreviations and terms

The glossary explains abbreviations and terms used in this pamphlet.

4. Summary of change

Specifically, this revision dated 23 October 2007 –

- Deleted section 6, paragraph e(2), in its entirety.
- Deleted section 6, paragraph e(5) in its entirety.
- Added section 4 "How to obtain a government user account."
- Changes all references from passwords to CAC (common access card).
- Changes password change time frame to new standards in section 5, paragraph c(1).
- Changes reference to information management officer (IMO) to system administrator (SA) and/or information assurance security officer (IASO).

5. Your government computer (GC)

a. Since almost all unclassified government computers (GCs) on Fort Hood are networked, your GC can reach or be reached by almost every unclassified GCs in Department of Defense (DOD). Because other DOD GCs trust your GC, you have access to DOD information not available to the general public. Additionally, almost all GC(s) on the LandWarNet (unclassified [unclass]) link to the commercial Internet. The LandWarNet (classified [class]), although not linked to the commercial Internet, is used to link DOD GCs together to share information classified up to Secret.

b. This internetworking of GCs makes your GC a gateway to vast amounts of information. It also exposes your GC to risks from all computers to which it can be linked. As a user of a GC on Fort Hood, you play a key role in protecting Fort Hood's data.

6. What is the threat?

Threats to your GC and the Fort Hood network can come from a virus, worm, hacker, or even a Soldier or DOD civilian in the military or United States (US) government.

a. Viruses and worms. Viruses and worms are programs that corrupt and damage programs, data, or both. A program does not have to perform malicious actions to be a virus or a worm; it only needs to infect or alter other programs. Most viruses; however, perform malicious actions, such as deleting data from your hard drive. Worms may manipulate a program on your GC that would allow a hacker free access to your data or use your computer as a "host" from which to infect other computers.

b. Opening an infected e-mail message or attachment from an unknown source is the most common method in which viruses spread today. You will never configure your computer to automatically preview e-mail messages.

c. Virus-hoax warnings are more common than actual viruses. Many virus and e-mail hoaxes use fake technical or emotional language and include suggestions for "get-rich-quick" schemes or heart-rending pleas, such as an "urgent" warning to pass along information to protect everyone from a devastating virus.

d. Deliberately introducing "malicious logic" (the technical term for viruses and other malicious programs) into any government information system is a violation of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ). Personnel not subject to the UCMJ may be subject to adverse action under United States Code (USC) and/or federal regulations. Hackers routinely attempt to exploit the security vulnerabilities found within software you run on your GC, often through the use of a virus or worm.

e. The best course of action is to prevent your GC from being infected in the first place. At Fort Hood, there are three things users can do to ensure their GC and information is adequately protected:

(1) Ensure the anti-virus software on your GC is current. Fort Hood policy requires your GCs anti-virus software be updated at least once each week. Anti-virus software must also be updated on all government-owned personal digital assistants (PDAs).

Note: In most organizations on Fort Hood, anti-virus updates are automatically “pushed” to GCs. Soldiers and DOD civilians may also load a copy of the DOD anti-virus program on their home computers.

(2) Be aware and report unusual computer activity listed in paragraph 9.

(3) *Log off* of your computer at the end of the day, *but do not turn the computer off.*

f. Even when taking the best precautions, viruses can still occur. They are not always immediately identifiable. Here are some things that may indicate the presence of a virus:

(1) Abnormal displays or banners appear on the computer screen.

(2) The computers performance slows down.

(3) The computer shows unusual activity or displays error messages, file sizes change, data, or programs are lost.

7. How to obtain a government user account

a. Your first step in obtaining a government user account is to contact your unit and/or organization IASO. The IASO will be able to provide you with all the required information.

b. If you have not already done so, you must apply and receive an Army Knowledge Online (AKO) e-mail account. All soldiers, Department of the Army Civilians (DACs), and in special situations, civilian contractors, are authorized to have an AKO account.

c. Read this pamphlet in its entirety; it will be utilized for taking the Fort Hood Computer User Test.

d. Arrange with your IASO to take and pass the Computer User Test.

e. Read and sign the Computer Users Agreement. Your IASO will provide this form to you.

f. You must have a valid CAC to access your user account at all times.

g. Remember, your use of a government computer system is not a right, but a *privilege*. You must adhere to all security guidelines at all times.

8. Using your government computer (GC)

a. Safeguarding GCs.

(1) The GC you are using is the property of the US government. GCs are to be used by government employees for official business, authorized personal use, and limited morale and welfare communications between deployed Soldiers and their Family members only. All users must:

(a) Safeguard each information system and its information against sabotage, tampering, denial-of-service, espionage, and release to unauthorized persons.

(b) Protect hardware, software, and documentation at the highest classification of the information residing on the information system.

(c) Report information system security incidents, vulnerabilities, and virus attacks to the SA or IASO.

(d) Check all magnetic media (for example, disks, compact disks (CDs), tapes, or universal serial bus (USB) memory sticks for malicious software [for example, viruses or worms]) before using it on a GC, information technology (IT) system, or network on Fort Hood.

(e) Check with your IASO to ensure that the system complies with the latest information assurance vulnerability message (IAVM) (for example, when taking a GC laptop home or when returning from temporary duty).

(2) Soldiers who fail to comply with this policy may be subject to adverse administrative action or punishment under Article 92 of the UCMJ. Personnel not subject to the UCMJ who fail to comply with these requirements are subject to disciplinary, administrative, or prosecutorial actions as authorized from criminal or civil sanctions under the USC or federal regulations.

b. Authorized personal use. Authorized personal use is defined by the DOD Regulation 5500.7 (Joint Ethics Regulation [JER]), paragraph 2-301, and AR 25-2, paragraph 4-5-r(6). This use includes brief access to, searches on the Internet, and sending short e-mail messages. The JER also requires commanders and supervisors to ensure that personal use of GCs does not adversely affect the performance of official duties. Personal use of GCs is authorized when it:

(1) Conforms to DOD and Fort Hood policies.

(2) Is of reasonable duration and frequency and, when possible, is done before or after normal duty hours.

(3) Does not create significant additional costs to DOD or the Army and does not reflect adversely on the DOD or the Army.

(4) Serves a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare.

(5) Employees may also be allowed to conduct job searches in response to downsizing. Using GCs to send e-mail between deployed Soldiers and their immediate Family members is authorized and strongly encouraged in the Army at Fort Hood.

(6) Does not overburden the military communication system. Remember, the military communication system, of which the LandWarNet (unclass and/or class) plays a vital part, is designed to support mission requirements of the war fighter.

c. CAC.

(1) Your CAC is one way of getting to the information highway. While your CAC opens a vast world of various military networks and the Internet, it can also allow others access to the same information. As a GC user on Fort Hood, you will have a unique CAC personal identification number (PIN) for the GC account you use. Maintaining the security of your PIN is therefore one of the most important security precautions you must take as a user. You alone are responsible for protecting your PIN and any e-mail messages that originate from your account. If someone obtains your PIN, they could

assume your identity in the virtual world. You are responsible for any activity that takes place on a GC under your log-on name and PIN. Do not share your PIN with anyone. The guidelines below will help you protect your CAC PIN:

- (a) Do not write down or post your PIN in your work area.
- (b) Do not store your PIN on-line or in a PDA or personal electronic device (PED) and do not include it in e-mail messages.
- (c) Make sure your PIN is not exposed on the screen when you log in.
- (d) Ensure your CAC is renewed prior to the expiration date. You will not be prompted by the systems in advance and will not be able to log on once the expiration date has passed.
- (e) If your account is on a classified network, your PIN is classified at the highest level of information on that network and you must protect it in the same manner as all classified information.

(2) Your PIN should not consist of your birthday, anniversary, or any other combination of numbers that someone can easily guess or determine.

d. Passwords for GCs that are not CAC enabled.

(1) Some GC systems have been placed in an enclave and therefore, still require a password to gain access to the Internet and/or information contained on the GC.

(2) Your password has the same authority and/or privileges as a CAC. As a GC user on Fort Hood with your GC located in the enclave, you will have a unique log-on name and password. You must maintain the same security standards of your password as described in section 8, paragraph c(1) above. Do not share your password with anyone. The guidelines below will help you protect your password:

- (a) Do not write down or post your password in your work area.
- (b) Do not store your password on-line or in a PDA or PED and do not include it in e-mail messages.
- (c) Make sure your password is not exposed on the screen when you log in.
- (d) Ensure your password is changed every 60 days on both the LandWarNet (unclass) and on the LandWarNet (class). If you know that your password is compromised, report to your SA for a new one.

(e) If your account is on a classified network, your password is classified at the highest level of information on that network and you must protect it in the same manner as all classified information.

(3) Your password can be either user-generated or issued by your SA/IASO. The following standards apply at Fort Hood:

(a) User account: Passwords must have at least 10 characters and include at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters. Passwords must not form a word or repeat any of the previous 10 passwords. If your password does not meet current Fort Hood standards, inform the SA immediately.

(b) Special privilege account passwords must be random, 15-characters, alphanumeric codes with at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters.

(4) Never leave your GC unattended while logged on unless the computer is protected by a "password-protected" screensaver.

e. Use of the LandWarNet (class).

(1) Any computer connected to the LandWarNet (class), which is a classified network, operates in at least the US Secret "system-high" mode. Any magnetic media used on the system and printed output must be marked and controlled immediately according to AR 380-5 (Department of the Army Information Security Program) until the data is declassified or downgraded by an approved process. In other words, any disk going into a secret system is now secret and must be handled accordingly. A "Secret" label must be placed on write-protected media. Classified North Atlantic Treaty Organization (NATO) material must be marked and controlled according to AR 380-5, chapter 4 and 5.

(2) You should not enter information into a system if the information:

(a) Has a higher classification than that for which the system is accredited.

(b) Is proprietary, contractor-excluded, or otherwise needs special protection or handling.

(3) If a system is connected to the LandWarNet (class), only US personnel with appropriate security clearance and a "need to know" will be allowed access to the system. Magnetic disks or diskettes must not be removed from the computer area without the approval of the local commander or head of the organization. The IASO should inform users of transient electromagnetic pulse surveillance technology (TEMPEST) requirements. TEMPEST (red and/or black) requires that system components be separated to prevent unauthorized monitoring. For this reason, the movement of hardware and other IT equipment must be approved by the IASO.

f. Use of public key infrastructure (PKI) certificates. If you have a PKI certificate installed on your computer (for example, a software token), you are responsible for ensuring that it is removed when it is no longer required. Commercial non-application softcerts are prohibited. If the certificate is no longer needed, you should notify your SA and the issuing trusted agent of the local registration authority.

g. Authorized software and hardware. Software and hardware used on a GC and the Fort Hood network must be licensed, accredited, and approved by your IASO, installation Information Assurance Manager (IAM), designated approving authority (DAA), and the Directorate of Information Management (DOIM) Computer Configuration Board (CCB). SAs will store the original software and licenses in a secure location, such as a locked cabinet or drawer. Only the DOIM and unit SA are authorized to install any software or hardware. Users are prohibited from processing government related work on employee-owned systems and from connecting personal computers to the Fort Hood network as well as connecting government systems to a commercial network.

h. Use of AKO. Soldiers, civilians, and DOD contractors who are authorized e-mail accounts at Fort Hood are required to have an AKO web-mail account. The use of all other web-mail services is prohibited for conduct of Army business communications.

AKO also provides the only authorized Internet chat service allowed on the LandWarNet (unclass and/or class). All other chat services are prohibited.

i. Prohibited web sites. Fort Hood filters web access to block users from accessing prohibited web sites (for example, those devoted to pornography and hate speech) and limit access for personal use. Authorized access may be obtained by exception. Contact your command IASO for assistance.

j. Prohibited activity. As a user, you are the first line of defense against unauthorized computer activity. The JER, section 3, AR 25-2, chapter 4, and Fort Hood's computer policy define prohibited computer software and computer-network misbehavior. The following is a summary (not prioritized) of this policy and prohibited activity on the Fort Hood network:

(1) Having or loading prohibited software onto GCs. Prohibited software includes peer-to-peer file-sharing software, such as moving picture experts group, audio player 3 (MP3) music and video software; streaming audio and video; moving picture experts group (MPEG) files; hacker tools and development software; malicious logic and virus-development software, executables, such as files with an ".exe" extension, and macros; network line-monitoring and keystroke-monitoring tools; unlicensed (pirated) software; web-page-altering software; games (including America's Army); personal firewalls, including DOD-licensed and Windows® XP Internet connection firewalls; and any other non-authorized software.

(2) Using networked IT or GCs for personal gain or illegal activities.

(3) Attempting to strain, test, circumvent, or bypass computer-network or security controls.

(4) Attempting to access data or use operating systems or programs, except as specifically authorized.

(5) Performing network line-monitoring or keystroke-monitoring without proper authorization.

(6) Modifying or tampering with the software or hardware on your GC.

(7) Moving a GC. Most damage to computers occurs when moving them. Contact your IASO for assistance.

(8) Introducing viruses, worms, or malicious codes into any IT or network.

(9) Sharing user identification or passwords.

(10) Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene material, such as racist, sexually explicit, harassing, or hate literature.

(11) Storing or processing classified information on a system (including PEDs and PDAs) not approved for classified processing.

(12) Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

(13) Unauthorized viewing of, changing, damaging, deleting, or blocking access to another user's files or communications.

(14) Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

- (15) Giving an unauthorized individual access to a government-owned or government-operated system.
- (16) Hacking into or from the Fort Hood network.
- (17) Sending or forwarding official e-mail from a GC connected to the LandWarNet (unclass and/or class) to a commercial Internet service provider (ISP) (for example, AOL®, CompuServe®, Hotmail®, Yahoo!®).
- (18) Using someone else's user identification and password or masking your own identity.
- (19) Writing or forwarding chain or hoax e-mail messages.
- (20) Posting personal homepages.
- (21) Using GCs for personal profit.
- (22) Downloading or loading freeware or shareware software.
- (23) Simultaneously connecting to the LandWarNet (unclass and/or class) and a commercial ISP.

k. Consent to auditing and monitoring.

(1) Auditing is defined as the independent review and examination of records and activities to assess the adequacy of system performance and controls, to ensure compliance with established policy and operational procedures, and to recommend necessary changes in controls, policy, or procedures. All transactions by users accessing the LandWarNet (unclass) or LandWarNet (class) are subject to audit.

(2) In general, Army members and employees use government communications systems with the understanding that any type of use, authorized or unauthorized, incidental or personal, serves as consent to monitoring. When you click "ok" on the warning banner that appears when starting a GC, you agree to have your GC monitored. GCs are monitored to ensure that use is authorized and that users follow security procedures. Among other things, monitoring is used for surveillance to reconstruct account activity, and to record attempts to bypass security mechanisms.

l. Minimize policy. During periods of heightened network security, DOIM may be forced to minimize non-mission essential activity on our networks.

9. Reporting computer security incidents

a. If you think that you have observed a computer security incident, you must report it to your SA or IASO immediately. A computer security incident is the act of violating an explicit or implied computer security policy. A few examples of computer security incidents are:

- (1) Attempts, either failed or successful, to gain unauthorized access to a system or its data (for example, hacking).
- (2) Attempts, either failed or successful, to defeat or circumvent computer network or security controls, such as altering the network configuration, or passwords.
- (3) Downloading MP3 files or other unauthorized software.
- (4) Writing or knowingly transmitting a virus, worm, or other form of malicious logic.
- (5) Forwarding chain e-mail messages.

- b. Additionally, immediately inform the SA or IASO if you think:
 - (1) Your GC has a virus.
 - (2) Your GC has been hacked or is being hacked.
 - (3) An authorized or required activity on the network is not functioning.
 - (4) Any *classified* spillage must be reported immediately.
- c. If you believe your GC is infected with a virus or worm or is behaving strangely, immediately take the following steps:
 - (1) Do not turn off your GC.
 - (2) Disconnect the network cable from the GC (the cable looks like a telephone cable).
 - (3) Call your SA or IASO. If they are unavailable, contact the DOIM Help Desk, your IAM, or a member of the Information Assurance Compliance Branch (IACB).

10. How to treat a government computer (GC)

You must treat your GC with care for it to function properly.

- a. Do not eat or drink near your GC. Spilling soft drinks, coffee, or other liquids on your computer can damage it and destroy your files.
- b. Keep your system clean and free of dust.
- c. Do not move your GC unless supervised by your SA or IASO.
- d. Lock workstations during brief periods of absence. Log off your GC at the end of your tour of duty, but do not turn off the system.
- e. Do not expose a GC to extreme heat, cold, or humidity.

11. Computer User Test

- a. Now that you have read and studied this guide, you are ready to take the Computer User Test. Log onto the IA Computer User Test web page at <https://ia.hood.army.mil/usertest.asp>.
- b. Your SA or IASO will require you to read and sign a FH Form 25-X33. Your signature acknowledges an understanding of and agreement to support Army and Fort Hood policy on the use of GCs. Your signature also makes you accountable for every transaction that occurs on your GC account. If you refuse to sign, you will not be given an account for any access to the Fort Hood computer network.
- c. From the moment you log on, you will enjoy the benefits of using a GC, but you will also face the responsibility that comes with it. There are hazards out there and you are responsible for protecting a GC and the network from those hazards by following proper procedures. Remember, this guide is a “driver’s manual.” Keep a copy near your GC or in an internal file.

12. Conclusion

As a user, you play a key role in protecting the integrity, availability, and confidentiality of data across Fort Hood and the Army’s computer network. Taking the steps listed above will help you ensure that your GC and all networks to which your GC is

connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the entire command. In summary:

- a. Guard your CAC PIN and/or password.
- b. Ensure anti-virus software is up-to-date on your GC.
- c. Follow the rules on personal use of your GC.
- d. Report viruses and all other network-security incidents to your SA or IASO.

23 October 2007

III CORPS & FH PAM 25-25

**Appendix A
References**

Section I. Required Publications

AR 25-2 (Cited in para 1, 8b, and 8j)
Information Assurance

AR 380-5 (Cited in para 8e(1))
Department of the Army Information Security Program

AR 380-67 (Cited in para 1)
The Department of the Army Personnel Security Program

Section II. Related Publications

DOD Regulation 5500.7
Joint Ethics Regulation

Uniform Code of Military Justice
Article 92

Section III. Prescribed Forms

This section not used.

Section IV. Referenced Forms

FH Form 25-X33
Computer User Agreement

FH Form 1853
Distribution Scheme

Glossary

Section I. Abbreviations

AKO

Army Knowledge Online

AOL

America Online

AR

Army Regulation

CAC

Common Access Card

CCB

Computer Configuration Board

CD

Compact Disk

CLASS

Classified

DAA

Designated Approving Authority

DAC

Department of the Army Civilian

DOD

Department of Defense

DOIM

Directorate of Information Management

FH

Fort Hood

GC

Government Computer

23 October 2007

III CORPS & FH PAM 25-25

GFE

Government Furnished Equipment

IA

Information Assurance

IACB

Information Assurance Compliance Branch

IAM

Information Assurance Manager

IASO

Information Assurance Security Officer

IAVM

Information Assurance Vulnerability Message

IAW

In accordance with

IMO

Information Management Officer

ISP

Internet Service Provider

IT

Information Technology

JER

Joint Ethics Regulation

MPEG

Moving Picture Experts Group

MP3

Moving Picture Experts Group, Audio Layer 3

NATO

North Atlantic Treaty Organization

NIPERNet

Unclassified, but sensitive Internet Protocol Router Network

PAM

Pamphlet

PDA

Personal Digital Assistant

PED

Personal Electronic Device

PIN

Personal Identification Number

PKI

Public Key Infrastructure

SA

System Administrator

SC

Signal Corps

SIPRNet

Secret Internet Protocol Router Network

TEMPEST

Transient Electromagnetic Pulse Surveillance Technology

UCMJ

Uniform Code of Military Justice

UNCLASS

Unclassified

US

United States

USB

Universal Serial Bus

23 October 2007

III CORPS & FH PAM 25-25

USC

United States Code

XP

eXPerience

Section II. Terms

Information technology (IT)

The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

LandWarNet (class)

The name of the Army's classified network. This term replaced SIPRNet.

LandWarNet (unclas)

The name of the Army's unclassified network. This term replaced NIPRNet.