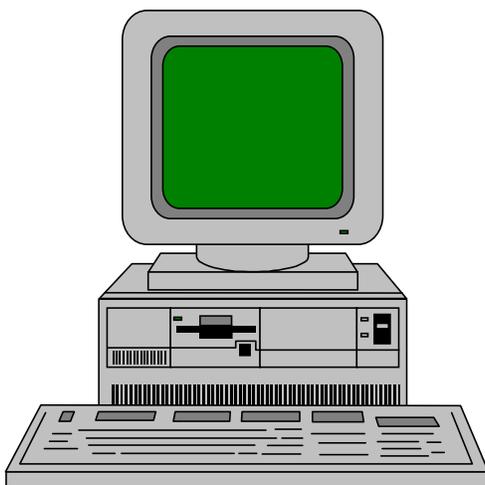


USAREUR Pamphlet 25-25

Information Management

USAREUR Computer-User Guide



**Headquarters
United States Army, Europe
and Seventh Army
Unit 29351
APO AE 09014**

17 March 2000

**Headquarters
United States Army, Europe
and Seventh Army
Unit 29351
APO AE 09014
17 March 2000**

USAREUR Pamphlet 25-25

Information Management

USAREUR Computer-User Guide

For the Commander:

CHARLES C. CAMPBELL
*Major General, GS
Chief of Staff*

Official:



JOHN P. CAVANAUGH
*Brigadier General, GS
Deputy Chief of Staff,
Information Management*

Summary. This pamphlet is a guide to using Government computers in the workplace. In support of information assurance, this guide prescribes procedures for using computers in a way that protects them against viruses and hackers.

Applicability. This pamphlet applies to all USAREUR military and civilian personnel who use Government computers in the workplace.

Forms. USAREUR and higher-level forms (printed and electronic) are available through the USAREUR Publications System (UPUBS) at <http://upubs.army.mil>.

Suggested Improvements. The proponent of this pamphlet is the Office of the Deputy Chief of Staff, Information Management, HQ USAREUR/7A (AEAIM, 380-5232). Users may suggest improvements to this pamphlet by sending a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, 5th Signal Command, ATTN: AFSE-IS (RCERT-E), CMR 421, APO AE 09056.

Distribution. A (UPUBS).

*This pamphlet is available at
<http://www.aeaim.hqusareur.army.mil/library/home.htm>.*

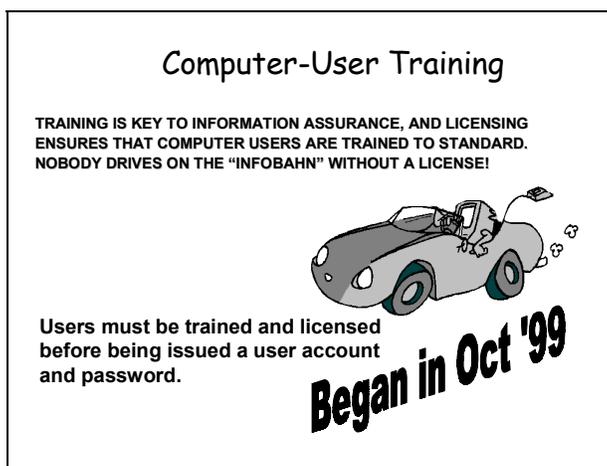
TABLE OF CONTENTS

	Page
1. Purpose.....	3
2. Your Computer as a Gateway to Information.....	3
3. What is the Common User Data Network and Internet Connectivity.....	4
4. How to Treat Your Computer.....	4
5. Personal Use of Your Government Computer.....	5
6. The Importance of Passwords.....	6
7. What are Viruses?.....	7
8. Detecting and Preventing Viruses.....	8
9. Chain-Mail, Virus Hoaxes, and Other Computer Hoaxes.....	10
10. Use of Hardware and Software.....	11
11. Reporting Computer-Security Incidents.....	11
12. Auditing Computer-User Activity.....	12
13. Monitoring.....	13
14. Prohibited Websites.....	13
15. MINIMIZE Policy.....	14
16. User Agreement.....	14
17. USAREUR Computer-User Test.....	15
18. Conclusion.....	15
Appendix	
A. USAREUR Computer-User Agreement.....	A-0
Glossary	Glossary

USAREUR COMPUTER-USER GUIDE

1. Purpose

As a USAREUR computer user, your actions can greatly increase or decrease the integrity, availability, and confidentiality of information concerning national defense. Protecting that information is called “information assurance.” This guide will help you understand and enforce information assurance by showing you how to recognize and avoid the hazards awaiting you once you enter the “infobahn.” This guide is your drivers manual for the infobahn. Before you can be issued a license to “drive,” you must take the USAREUR Computer-User Test (para 17) and sign the User Agreement. This guide tells you everything you need to know to pass the test.



2. Your Computer as a Gateway to Information

Since almost all unclassified USAREUR computers are networked, your computer has access either through your local area network (LAN) or over the Internet to almost every unclassified computer in the entire Department of Defense (DOD). This internetworking of computers makes your computer a gateway to vast amounts of sensitive but unclassified information. The security of our networks is only as strong as the weakest link. As a user of a computer in USAREUR, you play a key role in ensuring the availability, confidentiality, and integrity of our data. Comply with the rules that follow, and you will not be the weakest link.

a. If you can get out, a hacker can get in. A basic premise of networked computing is that if you have access to the Internet through your computer, hackers have access to you. Remember, the infobahn is a two-way street.

b. Since your computer is “trusted” by other computers within the military domain, it provides access to various military networks. “Trusted” means that other computers recognize your computer as a Department of the Army computer. As such, you can obtain passwords and gain access to certain information not available to non-Army users. Based on that, your actions can put your computer, your unit’s network, and all Army computer networks at risk. Your use of an Army computer therefore places a great deal of responsibility on your shoulders. You are directly responsible (along with others) for the security of the Army’s computer networks.

3. What is the Common User Data Network and Internet Connectivity

The Common User Data Network (CUDN) is a data network created for USAREUR that is intended for transmission of only unclassified information. We use the CUDN to communicate in Europe. The CUDN is linked to the World Wide Web (the Internet). We therefore need to know who has access to the CUDN to protect ourselves against hackers. This is why we cannot allow users to create “backdoors” to the Internet through the CUDN. A “backdoor” is an unauthorized, unknown connection between the CUDN and the Internet. If, for instance, your computer is connected to the CUDN through a LAN, simultaneously connecting to the Internet through a modem to a commercial Internet service provider creates a backdoor, which is prohibited.

4. How to Treat Your Computer

a. Your computer is an important part of the toolkit you need to do your job. You therefore must treat your computer with care. One of the most important things you must do is keep the temperature and humidity correct in your office. Heat is your computer’s worst environmental enemy. Exposing your computer to heat will shorten its lifespan and put your data at risk.

b. Do not eat or drink near your computer. Spilling soft drinks, coffee, or other liquids on your computer can damage it and destroy your files.

c. Keep your system clean and free of dust.

d. Do not disconnect your computer from its network. The small network connections are very fragile and very expensive.

e. Do not move your computer unless supervised by your system administrator (SA) or information systems security officer (ISSO). Most damage done to computers in the Army occurs while moving them. Computers also wind up missing after moves; so care must be taken to notify the hand-receipt holder of the computer's new location.

f. Turn your computer off at the end of the day. If your computer is turned off, it cannot be hacked. This also reduces the chance of a fire.

g. In many ways, you as a user can cause the biggest threats to your computer. Take care of your computer by following the above instructions and your computer will perform its many valuable functions for you day after day.

h. Change the default homepage on your Internet Explorer to a local file, to your unit's homepage, or to a server that is local to your community.

5. Personal Use of Your Government Computer

We have detailed rules for appropriate and inappropriate use of Government computers. We also have rules governing how you may use your Government computer for personal use. The U.S. Government provides you a computer to do your assigned duties. The taxpayer is not required to provide you free and unlimited Internet access. The rules are simple and clear. Government computers may be used only by Government employees for the following:

- Official business (a below).
- Authorized personal use (b below).
- Limited morale and welfare communications between deployed soldiers and their family members (c below).

a. Official business is that which is related to your official duties.

b. Authorized personal use is defined in the Joint Ethics Regulation (JER). Authorized personal use includes brief access and searches for information on the Internet and sending short e-mail messages.

c. The JER also requires commanders and supervisors to make every effort to ensure that personal use of Government computers—

(1) Does not adversely affect the performance of official duties.

(2) Is limited to reasonable durations and frequency and, when possible, done during off-duty hours.

(3) Serves a legitimate public interest, such as furthering the education and self-improvement of employees, improving employee morale and welfare, or job-searching in response to downsizing. Using Government computers to send e-mail between deployed soldiers and their immediate family members is authorized and strongly encouraged by USAREUR.

d. Personal use of Government computers must not overburden the communication system. Remember, in USAREUR the communication system is designed to support the warfighter.

e. Personal use of Government computers must not reflect adversely on DOD or DOD components. The JER specifically prohibits using Government computers for pornography, chain-mail, personal gain, or any action that violates another statute or regulation.

f. Other misuse of Government computers includes hacking or using hacker tools, visiting hacker websites, deliberately installing viruses on DOD computers, trying to mask or hide your identity, attempting to bypass security policy, and using Internet telephony, "streaming" audio/video websites (for example, keeping a webpage open to receive hourly stock updates).

g. Penalties for misuse of Government computers range from courts-martial to nonjudicial and administrative actions, such as letters of reprimand.

6. The Importance of Passwords

a. Your password is the key that gets you onto the information highway. While this key opens the vast world of various military networks and the Internet, it can also allow others access to the same information. Maintaining the security of your password is therefore one the most important security precautions you must take as a user.

b. The security of your password is important to maintaining the integrity of our networks. If your password is compromised, a computer intruder can access all data to which you have access. You should not write down your password, nor should you ever share your password with anyone. If someone obtains and uses your password, they could become "you" in the virtual world. You are responsible for anything that occurs on the network under your log-on name and password. If you share your password and someone logs on as you and then hacks a website or downloads a hacker tool, you could be held responsible.

c. As a computer user in USAREUR, you will have a unique log-on name and password for each computer account you use. USAREUR policy requires passwords to be at least eight digits long, include at least two numbers, and not form a word. You may not tamper with your computer to avoid the USAREUR password policy. Passwords must be changed every 6 months on unclassified systems, and every 3 months on classified systems. Do not configure a shared directory without password protection. This would enable everyone with access to the shared computer to modify, delete, or download your files. No group passwords are authorized unless the user's ISSO approves; the ISSO grants approval only for operational requirements.

d. Passwords that do not conform to the standards in c above are very vulnerable to password-cracking programs continually used by hackers. Most cracker programs compare passwords to words in dictionaries. If your password is made up of words or acronyms, the program unscrambles your password and gives the hacker access to your computer. Once hackers gain access to your computer, they have access to much of the DOD network. Password protection is therefore essential.

7. *What are Viruses?*

a. Computer viruses are programs that corrupt and damage programs and data. A program does not have to perform malicious actions to be a virus; it only needs to infect other programs. Almost all viruses, however, perform malicious actions. Deliberately introducing "malicious logic" (the technical term for viruses and other malicious programs) into any Government information system is a Federal crime for any soldier, DOD employee, or contractor. Withholding information needed to effectively implement countermeasures or antivirus protection is also against the law.

b. How do viruses get into your computer? Viruses can invade a system through any normal means of communicating, transferring, or sharing information (for example, through diskettes, CD-ROMs, modems, network interfaces, communication ports). The most common means of spreading a virus is through e-mail. Viruses that are spread through e-mail are inserted into files, which are sent as e-mail attachments. Remember that the virus is not in the body of the e-mail; it is in the attachment. Opening the attachment releases the virus. This is the most common method of spreading new viruses; users therefore need to be very careful when receiving e-mail attachments. Some viruses compromise the confidentiality of data and clog the e-mail system, hindering the availability of data. Other viruses use personal address books to spread. When, for example, a user opens an infected e-mail attachment, the virus sends the attachment to the first 50 addresses in the user's address book. More recent and more destructive

viruses erase a variety of files, including Word documents, Excel spreadsheets, and PowerPoint slides.

c. Many macro viruses exist. They are written for Word macro language and are spread through Word documents. This is a very serious problem, since we exchange so many Word documents by e-mail; as soon as the attached document is opened, the virus is activated. The more creative macro viruses use your personal address book or in-box to rapidly spread the virus by e-mail. The Melissa virus was spread worldwide in a matter of days. The speed at which new viruses can be spread by e-mail can cripple an entire e-mail system by generating more messages than the system can handle. If you receive an e-mail message with a suspicious attachment, scan the attachment for viruses before opening it. If you are still concerned, do not open the attachment; instead, contact your ISSO.

8. Detecting and Preventing Viruses

a. We have talked about viruses and what they can do once they have infected your computer. The best course of action is to prevent them from infecting your computer in the first place. Here are some things you can do:

(1) Make sure your system boots from the hard drive first.

(2) Use the current, DOD-authorized version of antivirus software. The Army uses Norton and McAfee. USAREUR policy requires you to update your computer's antivirus software once a week. (Exchange Servers must be updated daily.) Set your computer to do this for you by programming it to perform a "live update" of your antivirus software once a week. Remember, those who create antivirus software are always one step behind those who are creating new viruses. The more often you update your antivirus software, the better.

b. 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.

(2) Your computer's performance slows down.

(3) Unusual activity, error messages, changes in file sizes, and loss of programs or data.

c. The above symptoms do not always mean that your computer has a virus. You need to be aware, however, of these abnormalities and report them to your ISSO as soon as they occur.

d. Installing antivirus software is easy and free. You can also download the antivirus software paid for by the Army and install it on your computer at home. Ask your SA or your ISSO about this, or use the Regional Computer Emergency Response Team, Europe (RCERT-E), webpage to get a free copy of the software (<http://www.rcerte.5sigcmd.army.mil>). If you load antivirus software yourself, have your ISSO check to ensure you installed it correctly. Set the live-update feature to run the virus-scanner at least once a week. If you set your live update for 1100 Tuesdays, set the virus-scanner to run at 1130 Tuesdays. That will ensure you have the most up-to-date antivirus software running your weekly scans. When you scan your computer for viruses, set your antivirus software to scan "all files." To do that, click on *Where & What*, then select *All files*. Also be sure to scan "all diskettes."

e. Diligent use of antivirus software by all users of Government computers is the best way to prevent damage to USAREUR networks and data by viruses. Antivirus software companies are constantly updating their product. If you, as a computer user, keep your antivirus software up-to-date, your chances of getting a virus are very low. If every user of USAREUR networks kept their antivirus software up-to-date, the number of viruses would drop dramatically. When a recent virus struck, our computer users were doing a very poor job updating their antivirus software. We therefore had thousands of reported cases of the virus. When a later virus hit, we had less than one hundred reported cases in USAREUR. By keeping your antivirus software up-to-date, you will most likely never suffer the problems caused by viruses.

f. If you find a virus, contact your help-desk or ISSO immediately. Prompt reporting of viruses can lessen their effect by giving security officers time to warn coworkers, who can then check their computers for the virus. If you have a new virus, chances are good that others in your organization will have the same virus. If your system is infected, first make sure you have the most current version of antivirus software. Then disinfect all files. If you are unsure how to use the antivirus software, get help from an expert. Improper use of the software may fail to find all viruses. If you have a virus, try to determine the source. The ISSO can then notify the sender, who can clean the virus and lessen the chance of further spreading the virus. Always re-scan to make sure all viruses have been eliminated. We will never be completely free of viruses, but with the correct measures, we can do a better job of controlling them. Update your anti-virus software frequently, scan all diskettes, and be sure not to open suspicious e-mail attachments.

9. Chain-Mail, Virus Hoaxes, and Other Computer Hoaxes

a. The Internet is constantly flooded with bogus information (for example, messages about potentially damaging viruses, notices that Bill Gates will send you money for forwarding e-mail to others, messages about people waking up in bathtubs filled with ice in strange hotels without their kidneys). While some real information may be mixed in with these hoaxes and urban legends, it is unlikely. The best course of action on receipt of these types of messages is to delete them without reading them. The premise behind a hoax is that it will stimulate the reader to get emotionally involved (for example, by making the reader angry, afraid, eager for money offered) and immediately forward the message to everyone the reader knows or can reach through a Global Address List. That creates "chain-mail," which in turn creates bottlenecks of electrons in our e-mail and other network servers, slowing them down. Chain-mail can even cause network servers to "crash." Because of this threat to our systems, you are strictly forbidden to forward hoax messages to anyone except your ISSO or to the RCERT-E. Remember, Bill Gates is not going to send you money if you forward an e-mail message to thousands of people; but the Army might take some of your money if you do.

b. Virus hoaxes are not real viruses, but they can be harder to get rid of than real viruses. Virus hoaxes and other e-mail hoaxes take up space on e-mail servers, use up network bandwidth, and waste time. Virus hoaxes are more common (and sometimes more time-consuming) than actual viruses. They usually take the form of e-mail warnings sent to large numbers of people to warn them about nonexistent viruses. Before you forward warnings such as these to the RCERT-E or to your ISSO, read the Hoaxes & Scams page on the RCERT-E webpage (<http://www.rcerte.5sigcmd.army.mil>).

c. If you receive a warning and are not sure if it is real, do not send it to everyone you know; forward it your ISSO. Here are some common hoaxes:

- Telephone Scam-Request to Forward
- Join the Crew
- Penpal Hoax
- AIDS Hoax
- Bill Gates \$1000 chain-mail
- Bill Gates/Windows 98 chain-mail
- Yahoo! World Domination Virus
- Win-a-Holiday
- Bud Frogs Screen Saver
- Tommy Hilfiger
- BUDDYLST.ZIP

d. When any of the items above are forwarded to large numbers of users, they use up bandwidth, take up space on e-mail servers, and mislead recipients. Forwarding chain-mail and hoaxes violates the JER and Army policy. Data networks were designed to support the warfighter in USAREUR; forwarding chain-mail does just the opposite by causing systems to overload and fail, thus putting our soldiers at risk by blocking their ability to communicate.

10. Use of Hardware and Software

a. Software. Software used on Government computers must be licensed, accredited, and approved by your organization. If you want to load private software on your Government computer, you must have the approval of your SA or ISSO. You may not load any games on your computer. All software on your computer must meet standards established in the USAREUR Computer Software Baseline (<http://www.rcerte.5sigcmd.army.mil>).

b. Hardware. Any hardware you use must be accredited. As the user, you must maintain property accountability. You cannot install and use your own hardware at work. Any hardware your unit buys must meet Army accreditation standards and be accounted for properly.

11. Reporting Computer-Security Incidents

a. Users must report any suspected individual computer-security incidents to their ISSO or, in the absence of the ISSO, to the organization's information systems security manager (ISSM). ISSOs report to ISSMs.

b. Users must report all network-security incidents to their ISSO. If you think you observed a network-security incident, report it to your ISSO and let the ISSO determine whether or not it requires further investigation.

c. Users are often the first in the command to recognize a new virus. Reporting viruses to your ISSO or ISSM as soon as you detect a virus will greatly increase the chances of catching and stopping the virus from spreading any further. Other users can be warned and, subsequently, update their antivirus

software and scan their system for any new viruses. Early reporting of viruses also gets the word to computer users not to open e-mail attachments that contain the virus; warnings such as these are the best way to limit the spread of viruses that are transmitted in attachments.

d. Users are also among the first to notice intrusions by hackers. Some indications of a possible intrusion are seeing a web-browser open on your screen without your having opened it, noticing your CD-ROM drive trying to read a compact disk (CD) without your prompting it, or finding that your files are mysteriously being deleted or moved. If any of these things are happening, you may be the victim of a hacker and must report the incident to your ISSO or ISSM immediately.

12. Auditing Computer-User Activity

a. 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.

b. Auditing has four goals:

(1) Review computer use.

(2) Reveal repeated attempts to bypass computer-protection mechanisms.

(3) Deter attempts to bypass security mechanisms and deter unauthorized use of computers.

(4) Provide a record of computer-user activity.

c. Auditing must allow for review of—

(1) Access patterns to individual files.

(2) Access histories of specific processes.

(3) Use and effectiveness of various protection mechanisms supported by the system.

d. Auditing records all known attempts to bypass security mechanisms. The ISSO needs assurance that auditing will identify attempts to gain access or

permission to system files or other restricted information on the system. The audit trail is a set of records containing the history of the activities occurring on a system. Audit trails provide multiple services. They are used to detect and deter penetration of a computer system and to reveal use that identifies misuse. Audit trails cover all applications on the system (for example, word-processing, e-mail, web-traffic, databases, access to shared directories). Audit trails also record events by date, time, user identity, location, and the file in use.

e. Official audits must be done by someone other than the user. Even the most secure system is vulnerable to attack. Auditing provides an excellent way of determining whether or not such attacks may take place and, if so, how.

f. Auditing allows your organization to perform two very useful security functions: surveillance and reconstruction. Surveillance is the monitoring of user activity. Surveillance includes log-ons and log-offs, remote-system access, logs of web-activity, opening and closing files, changes in privileges, changes in security attributes, and changes in user access. If the audit program is configured correctly, the ISSO will be able to reconstruct all activity during specific times by specific users.

13. Monitoring

Your use of a Government computer constitutes consent to monitoring. When you click OK on the warning banner, which opens when you start your computer, you are giving your consent to having your computer monitored. Your Government computer is provided to you for authorized use only. Government computers are monitored to ensure that use is authorized and that users follow security procedures. Monitoring is also done to see if hackers have gained access to computers. Privacy does not exist on Government computers; users should therefore not expect it.

14. Prohibited Websites

a. USAREUR has blocked users from accessing certain websites (for example, those devoted to pornography and hate speech). A large number of non-mission-essential websites in various geographic regions (for example, Iraq, Serbia) have also been blocked. Remember, the USAREUR telecommunications network is intended primarily to support the warfighter; personal use of Government computers hinders that support by overburdening the system. The CUDN sometimes has a hard enough time as it is handling all authorized data, without having to accommodate personal web surfing.

b. If you want access to a blocked website, you may request access by calling the Theater Network Operations Center (TNOC), 5th Signal Command, at 380-4444. Be prepared to fully justify your request. When contacting the TNOC, give the TNOC the uniform resource locator (URL) of the blocked website. The TNOC will view the site and determine whether to leave it blocked or to unblock it. If you disagree with the TNOC's decision, you may appeal through your chain of command.

15. MINIMIZE Policy

When a *MINIMIZE* order is issued to all users of USAREUR computer networks, all personal use of Government computers is prohibited for the duration of the order, except for the following:

a. E-mail messages between deployed soldiers and their families. Units are encouraged to make office computers available to family support groups for supervised use of Government networks for e-mail exchanges with soldiers deployed in support of United Nations, North Atlantic Treaty Organization, and United States European Command missions.

b. Computer use required for Army or other authorized education-center training or programs leading to college degrees.

c. Morale, welfare, and recreation activities.

d. Department of Defense Dependents Schools activities, provided student activity is monitored by adult supervisors.

16. User Agreement

Appendix A is an agreement between you and the U.S. Government concerning use of Government computers. Before you log onto your computer, you will be required to read and sign the agreement. Your signature acknowledges your understanding of and agreement to support Army and USAREUR policy on the use of Government computers. Your signature also makes you accountable for every transaction that occurs on your computer account. Your ISSO or SA will download a copy of the agreement from the RCERT-E webpage and ask you to sign it before issuing you a password. If you refuse to sign, you will not be given access to USAREUR computer networks.

17. USAREUR Computer-User Test

a. Now that you have read the guide, you are ready to take the USAREUR Computer-User Test. To do so, log onto the Information Assurance Computer-User Test Web-page at <http://ia-test.hqusareur.army.mil>.

b. Once you have taken and passed the test, you will be issued a USAREUR Information Assurance Computer-User License that authorizes you to “drive” on the “infobahn.” Your SA will then issue your computer-user account. From the moment you log on, you will enjoy the benefits of access, but you will also be faced with the responsibilities that come with it. There are hazards out there on the infobahn, and you are responsible for protecting your computer and your network from those hazards by following proper procedures. Remember, this guide is your “drivers manual.” Keep a copy near your computer or in one of your internal files.

18. Conclusion

a. As a USAREUR computer user, you play a key role in protecting the integrity, availability, and confidentiality of USAREUR data. To recap:

- Guard your password.
- Follow the rules on personal use of your computer.
- Never forward chain-mail or computer hoaxes.
- Keep your antivirus software up-to-date.
- Report viruses and all other network-security incidents to your ISSO.

b. Taking the steps listed above will help you ensure that your computer and all networks to which your computer is connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the entire command.

**APPENDIX A
USAREUR COMPUTER-USER AGREEMENT**

This appendix is a copy of the USAREUR Computer-User Agreement on the Regional Computer Emergency Response Team, Europe, webpage at <http://www.rcerte.5sigcmd.army.mil>. Your system administrator or information systems security officer will ask you to sign a copy of this agreement before issuing you a password.

As a user of a USAREUR automated information system, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any Government-owned software or install hardware on any Government-owned computer (for example, client-workstation, server) without first getting written approval from my system administrator (SA) or information systems security officer (ISSO).
3. I will not try to access data or use operating systems or programs, except as specifically authorized.
4. I know I will be issued a user identifier and a password to authenticate my computer account. After receiving them—
 - a. I will not allow anyone else to have or use my password. If I know that my password has been compromised, I will report to my SA for a new one.
 - b. If my account is on a classified network, I understand that my password is classified at the highest level of information in that network, and I will protect it in the same manner as that information.
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on, as long as I am the sole user of the account and the account is protected by a password that is know only by me.
 - d. If I have a classified account, I will ensure that my password is changed at least once every 3 months or when compromised, whichever is sooner.

e. If I have an unclassified account, I will ensure that my password is changed at least twice a year or when compromised, whichever is sooner.

f. I understand that if my password does not meet current USAREUR standards (for example, length, character set, no prohibited sequences or combinations), I am to inform the SA.

g. I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the ISSO.

h. I will not tamper with my computer to avoid adhering to USAREUR password policy.

i. I will never leave my classified computer unattended if it is a classified system while I am logged on or while the computer is unprotected by a "password protected" screensaver.

5. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

6. I know that if connected to the Secure Data Network (SDN), my system operates at least in the U.S. Secret, "system-high" mode.

a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until 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.

b. I must protect all material printed out from the SDN at the system-high level until I or someone with the appropriate clearance personally reviews and properly classifies the material.

c. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the ISSO.

d. If connected to the SDN, only U.S. personnel with a security clearance are allowed unescorted access to the system.

e. Magnetic disks or diskettes will not be removed from the computer area without the approval of the local commander or head of the organization.

7. My local ISSO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the SA or ISSO.
8. I will check all magnetic media for malicious software (that is, viruses) before loading it onto a USAREUR system or network.
9. I will not forward chain-mail or virus warnings. (The Regional Computer Emergency Response Team, Europe, issues virus alerts and threat advisories.) I will report chain-mail or virus warnings to my ISSO and delete the message. I will not attempt to run "sniffer" or other hacker-related software on the system.
10. I know I am subject to disciplinary action for any abuse of access privileges.
11. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site ISSO. I know what constitutes a security incident and know that I must immediately report such incidents to the ISSO.
12. I will comply with security guidance issued by my system administrator and ISSO.

I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, SA, or ISSO, I will ensure that all users in my area of responsibility sign this agreement.

Name (typed or printed): _____ (Use the RCERT-E webpage version)

Signature: _____ (Use the RCERT-E webpage version)

Date signed: _____ (Use the RCERT-E webpage version)

GLOSSARY

Abbreviations

CD	compact disk
CD-ROM	compact disk, read-only memory
CUDN	Common User Data Network
DA	Department of the Army
DOD	Department of Defense
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
ISSM	information systems security manager
ISSO	information systems security officer
JER	Joint Ethics Regulation
LAN	local area network
RCERT-E	Regional Computer Emergency Response Team, Europe
SA	system administrator
SDN	Secure Data Network
TNOC	Theater Network Operations Center, 5th Signal Command
URL	uniform resource locator
U.S.	United States
USAREUR	United States Army, Europe

Terms

For explanations of terms used in this pamphlet, see your servicing system administrator, information systems security manager, or information systems security officer.