Headquarters
United States Army Europe and Seventh Army
United States Army Installation Management Command
Europe Region
Heidelberg, Germany

Army in Europe
Pamphlet 25-25*

7 May 2009

Information Management

Army in Europe Information Technology Users Guide

***This pamphlet supersedes AE Pamphlet 25-25, 2 June 2006.**

For the Commander:

BYRON S. BAGBY
Major General, US Army
Chief of Staff

Official:

HEADQUARTERS, UNITED STATES ARMY, EUROPE AND SEVENTH ARMY

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This pamphlet is a users manual that provides guidance on authorized and secure use of information technology in the Army in Europe. It provides procedures for using Government computers (GCs) in a way that protects Army information systems against threats to the confidentiality, integrity, and availability of the information that is stored on as well as processed and transmitted by those systems. This pamphlet also serves as the study guide for users preparing to take the Army in Europe Information Systems User Test, which the user must pass before being issued system and network login credentials.

Summary of Change. This revision changes the name of—

● The Computer-User Test to the Information Systems User Test.

● The Computer-User Agreement to the Acceptable-Use Policy Agreement.

● The USAREUR Automation Training Program to Army in Europe Information Technology Training (AE-ITT) and provides a new URL for the AE-ITT website.

Applicability. This pamphlet applies to military and civilian (DOD, contractor, and non-U.S.) personnel in the Army in Europe who use a GC. This includes contractor-owned computers that are explicitly authorized by contract to connect to Army in Europe networks or to conduct Government business.

Forms. AE and higher level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this pamphlet must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this pamphlet is the USAREUR G6 (AEAIM-I, DSN 379-6254). Users may suggest improvements to this pamphlet by sending DA Form 2028 to the USAREUR G6 (AEAIM-I), Unit 29351, APO AE 09014-9351.

Distribution. A (AEPUBS).

CONTENTS

1. PURPOSE

As a user of a Government computer (GC), your actions have a significant and direct effect on the security of Army networks. This pamphlet provides an overview of the cyber-threats you will face and the rules designed to protect Army information. Careful study of this pamphlet will help you pass the Army in Europe Information Systems User Test (ISUT). After you pass the ISUT, you will need to read, agree to, and sign the Army in Europe Acceptable-Use Policy Agreement, which requires you to comply with the fundamental principles of information assurance (IA). Passing the ISUT and signing the Acceptable-Use Policy Agreement are both required before you can be issued computer and network login credentials.

2. REFERENCES

a. Publications.

(1) DOD 5500.7-R, Joint Ethics Regulation (JER).

(2) AR 25-1, Army Knowledge Management and Information Technology.

(3) AR 25-2, Information Assurance.

(4) AR 25-55, The Department of the Army Freedom of Information Act Program.

(5) AR 380-5, Department of the Army Information Security Program.

(6) AE Regulation 25-1-5, Public Key Infrastructure (PKI).

b. Form. DA Form 2028, Recommended Changes to Publications and Blank Forms.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. THE THREAT

a. Our warfighting capability depends to a great extent on the confidentiality, integrity, and availability of Army information and of the information systems (ISs) that store, process, and transmit that information. Proper protection of that information and those systems gives users an edge in the battle for information superiority by enabling them to make timely and effective operational decisions. These systems are being attacked every day. External threats range from casual hackers and virus developers to State-sponsored cyber-terrorists. Internal threats include malicious and unintentional actions by members of our own workforce.

b. Almost all GCs that store, process, and transmit unclassified and sensitive information are networked. Your GC can therefore reach—and be reached by—almost every unclassified GC in DOD. Furthermore, the NIPRNET (pronounced *nipper net*) is linked to the commercial Internet. Although the SIPRNET (pronounced *sipper net*) is not linked to the Internet, it is linked to other DOD networks to enable the sharing of information classified up to and including U.S. Secret and NATO Secret. This makes your computer a gateway to vast amounts of information, much of which is sensitive and not releasable to the public. It also exposes your GC to risks from all computers to which it can be linked.

c. Our best defense against these threats is the application of sound IA procedures by a trained, aware, and vigilant workforce. Commanders have the lead in ensuring our IA posture is kept at an acceptable level, but they need the help of every Soldier and civilian in the Army in Europe. Remember that an information-security risk accepted by one is a risk imposed on everyone. As a GC user in the European theater, you play a key role in protecting our data.

5. MINIMIZING THE RISK

The following are some ways to reduce risks to information security:

a. Consent to Auditing and Monitoring. Soldiers, employees, and contractors use Government communications systems with the understanding that any type of use (authorized or unauthorized, incidental or personal) serves as consent to auditing and monitoring. When you click “OK” on the warning banner that appears when you start your GC, you are agreeing to have your activity monitored for compliance with applicable IA policy. If you do not click “OK,” you will not gain access to the system. Authorized real-time monitoring and audit-log reviews enable account activity to be reconstructed, which in turn reveals successful and unsuccessful attempts to violate policy or bypass security controls. However, consent to interception or capture and seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law-enforcement or counterintelligence investigations against any party, monitoring of content, privileged communications or data (including work product), and does not negate any applicable privilege or confidentiality that otherwise applies. Personal representation or services by attorneys, psychotherapists, or clergy and their assistants are communications and work products that are private and confidential.

(1) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined according to established legal standards and DOD policy. Users are strongly encouraged to seek personal legal counsel on these matters before using an IS if the user intends to rely on the protections of a privilege or confidentiality.

(2) The user should take reasonable steps to identify these communications or data that the user asserts are protected by privilege or confidentiality. The user's identification or assertion of a privilege or confidentiality, however, is not sufficient to create this protection where none exists under established legal standards and DOD policy.

(3) Failure to take reasonable steps to identify communications or data as privileged or confidential does not waive the privilege or confidentiality if this protection otherwise exists under established legal standards and DOD policy. In these cases, the U.S. Government is authorized to take reasonable actions to identify communications or data as being subject to a privilege or confidentiality. These actions do not negate any applicable privilege or confidentiality.

(4) These conditions preserve the confidentiality of the communications or data, and the legal protections regarding the use and disclosure of privileged information. These communications and data are therefore private and confidential. Further, the U.S. Government will take all reasonable measures to protect the content of captured or seized privileged communications and data to ensure they are appropriately protected.

b. Authorized Use. Your GC is the property of the U.S. Government (or, in some cases, the property of a Government contractor as part of a contract requirement), as is any output from the computer (for example, printed official documents). These systems are to be used only by Government employees or Government contractors for official and authorized purposes (including explicitly authorized but limited unofficial or personal use). Users may gain access to data and use operating systems and programs only as specifically authorized, and will not attempt to strain, test, or bypass computer and network security controls.

(1) AR 25-2 requires everyone who uses or has access to Government networks to be assigned an appropriate information technology (IT) level. The determination of your IT level must be supported by an appropriate background investigation. This requirement applies to all networks (even those not normally requiring security clearances) and users, including interns and summer hires. Your information assurance manager (IAM) will assist in determining what IT level is required and coordinate with the G2 or S2 (security manager) to initiate the necessary paperwork to begin the required background check.

(2) "Authorized personal use" is defined by the Joint Ethics Regulation (JER) (DOD 5500.7-R) and AR 25-1. This use includes brief, unofficial access to and searches on the Internet and sending short e-mail messages. It does not include personal business use. 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—

(a) Conforms to DOD, Army, and Army in Europe IA policy.

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

(c) Does not create significant additional costs to or reflect badly on DOD or the Army.

(d) Serves a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare. Units are encouraged to make GCs available to Family readiness groups for supervised use of Government networks to exchange e-mail with Soldiers deployed in support of United Nations, NATO, USEUCOM, and other U.S. Forces missions. Employees may also be allowed to conduct job searches in response to downsizing.

(e) Does not overburden the military communication system. Remember, the military communication system is designed to support the mission requirements of the warfighter.

(3) All military personnel, Government civilians, and contractors who work for the U.S. Army and are authorized e-mail accounts are required to have an Army Knowledge Online (AKO) webmail account. Commercial webmail services (for example, America Online (AOL), Hotmail, Yahoo) are prohibited for official Army communications. AKO also provides the only authorized Internet chat service allowed on the NIPRNET. All other chat services are prohibited. U.S. supervisors will sponsor contractors and host-nation civilians for AKO accounts.

(4) To help ensure that use of the Internet on Army in Europe networks is authorized and appropriate, USAREUR has implemented Blue Coat, a program that blocks users from accessing prohibited websites (for example, those devoted to hacking, hate speech, or pornography) and may limit access for personal use. Contact your IAM for assistance if you believe you need special access to a blocked site.

(5) During periods of heightened network activity, the Army in Europe may be forced to minimize non-mission-essential activity on our networks. When a “minimize order” is issued to all users of computer networks, all personal use of GCs on Army in Europe networks is prohibited for the duration of the order, except for the following:

(a) E-mail messages between deployed Soldiers and their Families.

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

(c) Morale, welfare, and recreation activities.

(6) The following is a summary (not prioritized or comprehensive) of prohibited activities on Army in Europe computer networks not specifically addressed elsewhere in this pamphlet:

(a) Using someone else’s user-ID and password or masking your identity.

(b) Giving an unauthorized individual access to a Government-owned or -operated system.

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

(d) Hacking into or from Army in Europe networks.

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

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

(g) Automatically forwarding official e-mail or sending official, sensitive e-mail from a GC connected to the NIPRNET to an e-mail account serviced by a commercial Internet service provider (ISP) (for example, AOL, Hotmail, Yahoo).

(h) Online gambling.

(i) Hosting personal homepages on a GC or on an Army in Europe network.

c. Special Considerations for Using the SIPRNET. The following are some of the special considerations when using the SIPRNET:

(1) You must not enter information into a system if the information has a higher classification than that for which the system is accredited, or if the information is proprietary, contractor-excluded, or otherwise needs special protection or handling.

(2) Only U.S. personnel with appropriate security clearances are allowed unescorted access to GCs connected to the SIPRNET.

(3) Uncleared persons (U.S. and non-U.S.) will not have access to areas where SIPRNET equipment is located. If an uncleared person is authorized temporary access to a U.S.-controlled area where SIPRNET equipment is located, he or she must be announced and escorted at all times, and computer screens must be covered. If an uncleared person is permitted to view a screen, appropriately cleared U.S. personnel who have authority to release such information must ensure that the information viewed may be disclosed to that individual. At no time will an uncleared person have control of a SIPRNET terminal.

(4) Do not bring any electronic device into a classified workarea unless specifically cleared to do so by the designated approving authority (DAA). This includes areas in which there is a protected distribution system (PDS) drop box, or where a talon card or tactical local area network encryption is being used, which can be used to temporarily connect a classified GC to the SIPRNET.

d. Authorized Software and Hardware. Software and hardware installed on a GC must be properly licensed. Its acquisition and use must be coordinated with your information assurance security officer (IASO) or IAM, and approved by the DAA. Major changes to a system or network also require approval by the DAA. Modifying or tampering with the software or hardware on your GC or moving your GC without consent of your information management officer (IMO), system administrator (SA), or IASO is prohibited. The physical security and accountability for the system can be jeopardized if the system hand-receipt holder and responsible security personnel lose visibility and control of the system.

(1) The individual in your organization responsible for controlling licensing, distribution, and installation of software should store original software in a secure location such as a locked cabinet or drawer. Contact your IMO, SA, or IASO for any software or hardware needs necessary to do your job; if approved, your IMO, SA, or IASO will install it and ensure security implications are considered.

(2) Prohibited software includes peer-to-peer file-sharing, music, and video-sharing software (for example, MP3, MP4, Moving Picture Experts Group (MPEG)); hacker tools and hacker software; malicious-code development software; network line-monitoring and keystroke-monitoring tools; unlicensed ("pirated") software; webpage-altering software; games (including "America's Army"); and personal firewalls (including DOD-licensed and Windows XP Internet Connection/Windows firewall, unless specifically authorized). Additionally, you must not obtain, install, copy, store, or use software if doing so would violate the vendor's license agreement, and you must not download or install freeware or shareware software on a GC or on Army in Europe networks unless approved by the DAA.

(3) Employee-owned ISs, including but not limited to computers, universal serial bus (USB) memory sticks, and other electronic media and devices, are prohibited on Army in Europe networks.

(4) Use of wireless technologies (especially 802.11/WiFi® wireless access points and wireless clients), including wireless network capabilities built into some computers and personal digital assistants (PDAs), requires approval of the DAA and the USAREUR G6 Information Assurance Program Manager (IAPM), Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A. Use of 802.15/Bluetooth wireless technology is prohibited. Contact your IASO or IAM for guidance before using such devices or acquiring them for use with Government networks. Of special concern are laptops with built-in wireless capability. If, for example, your system has an Intel® Centrino® processor, it will almost certainly have a built-in wireless network card and you may be unaware when the wireless card is active. This can open a "backdoor" to your system and to Army in Europe networks and allow exploitation by hackers. If your computer has such a processor or if you are unsure if it does, ask your SA or IASO to verify. This is especially critical for systems connected to the SIPRNET, where any use of unapproved wireless devices may allow unauthorized access to classified information and ISs. If you receive authorization to bring an unclassified electronic device into a classified area (or an area where a SIPRNET PDS drop box is located), you must ensure that its wireless functionality has been disabled.

(5) To prevent opening a backdoor to hackers, never install or attach a modem to a GC or an Army in Europe network without approval from the DAA, nor simultaneously connect your GC to a Government network and commercial ISP.

e. Protecting Your Computer and Information—Physical and Document Security. Users must safeguard computers and information against theft, sabotage, tampering, denial of service (DOS), espionage, and release to unauthorized persons.

(1) You must treat your GC with care for it to function properly. Here are some rules:

(a) Do not eat or drink near your GC. Spilling soft drinks, coffee, or other liquids on your GC can damage it and destroy your files.

(b) Do not expose your system to potentially harmful environmental conditions such as extreme heat, cold, humidity, or dust.

(c) Never disconnect your GC from its network-connection box (switch or hub) unless specifically approved and supervised by your IMO, SA, or IASO. Exceptions to this rule may exist if your classified system is temporarily connected to the SIPRNET at a PDS drop box. (See your SA or IASO if you have questions.)

(d) Never turn off your GC at the end of the duty day or before going on leave or temporary duty (TDY). You should always log off of your computer, but the GC must remain on. The monitor should be turned off. The GC must remain on overnight to install security patches to the system during nonduty hours, which prevents inconvenience to users during the duty day. If your GC is turned off, it cannot be patched and therefore represents a significant vulnerability to security of Army in Europe networks, the LandWarNet, and the Global Information Grid. Additionally, it prevents the organization from meeting regulatory reporting requirements for information assurance vulnerability alerts and Federal Information Security Management Act compliance.

(2) Protect hardware, software, and output by properly labeling printed and electronic documents or media at the highest classification of the information stored on the computer or, if connected to a network, the highest classification of the network. If you are in a mixed environment area (having simultaneous access to the NIPRNET and SIPRNET), all media must be marked Unclassified, For Official Use Only (FOUO), Confidential, or Secret, as appropriate. The marking and control of classified output and media must be done according to AR 380-5; this also applies to declassifying or downgrading the information. In other words, any digital storage media inserted into a Secret system automatically becomes Secret and must be handled accordingly. Classified computers, documents, and other media must not be removed from a classified workarea without the approval of the local commander or head of the organization. Check with your security manager or IASO to determine if classified courier orders are required before transporting classified material from one area to another, and for instructions on proper packaging of items for transport.

(3) Unless you work in an approved open-storage area, you must lock classified devices, media, and output in an approved security container when not using them.

(4) In classified workareas in which unclassified systems or network cables are located (including normally unclassified areas where a SIPRNET connection is available through a PDS drop box), you must ensure that TEMPEST (Red/Black) requirements are met. TEMPEST procedures ensure that unclassified and classified system components and communication links are appropriately separated to prevent the electronic “leakage” or transfer of classified but unencrypted data from the SIPRNET to the NIPRNET. The danger of leakage also exists if other unclassified electronic devices are brought into areas where classified systems or networks are present. Devices such as these may be brought into these areas only if approved by the DAA. If you are not sure of the possible TEMPEST requirements in your area, ask your IASO.

(5) Laptops taken by the user on missions away from the office are particularly susceptible to theft. You must be aware that anyone having physical access to your system (whether through theft or simply walking into your office while you are out) can, with the right hardware and software tools, easily take control of your GC and steal, delete, or manipulate your data. All laptops that are used for traveling must be in compliance with Army and Army in Europe data-at-rest (DAR) encryption requirements (para 7).

f. Protecting Your Password. Your common access card (CAC) along with your personal identification number (PIN) is the standard method to access your system. If your CAC is in your system’s CAC reader, remove it and take it with you when leaving your GC unattended. If granted an exception to use a username and password combination to login to a GC, you will have a unique login name and password for each account you use. Because your password grants access to Army in Europe networks and the Internet, protecting it prevents others from gaining the same access by assuming your identity. Remember, you are responsible for any activity that takes place on a GC under your login name and password, including any e-mail messages that originate from your account. Protecting your password is therefore one of the most important security measures you must take as a user. Use the following guidelines to protect your password:

(1) Do not share your password or CAC PIN with anyone.

(2) Do not write down or post your password in your workarea.

(3) Do not store your password online, in a PDA, on any other personal electronic device (PED), or in any other media; and do not reveal your password to anyone in e-mail messages.

(4) Ensure your password is not exposed to others on the screen when you log in. (Normally this will be handled by the computer operating system.)

(5) Never leave your GC unattended while logged on unless the system has a password-protected screensaver that is set to activate after no more than 10 minutes of inactivity. Although this setting provides some level of security, the best practice is to activate the password-protected screensaver every time you leave your computer by pressing the *Ctrl-Alt-Del* keys (at the same time) and then selecting *Lock Computer*.

(6) If your password is compromised, you must report this to your SA immediately so that your account can be locked and the password changed.

(7) Ensure your password is changed every 90 days for NIPRNET accounts and every 60 days for SIPRNET accounts. Normally, your computer operating system will notify you when your password is about to expire.

(8) 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 accordingly.

(9) Your password can be either user-generated or issued by your IMO. The following standards apply:

(a) User-generated passwords must have at least 14 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 your last 10 passwords. If your password does not meet current standards, you should inform your SA immediately. Normally, your system will not accept passwords not meeting these requirements.

(b) IMO-issued passwords must be random, unique, and have the same length and complexity as user-generated passwords. They also must be changed on first logon.

(10) If your account is no longer needed or if you transfer to another organization, you must report this to your SA.

(11) Never use the same username or password that you use at work for any home accounts, e-mail, or websites.

g. Defending Your Computer Against Viruses. Viruses and worms are programs that may corrupt and damage applications, data, or both. Although a program does not have to perform malicious actions to be a virus or a worm, most malicious code (the generic term for this type of program) does perform harmful actions such as deleting data from your hard drive. Worms may manipulate a program on your GC and provide a hacker access to your data or to use your computer as a “host” from which to infect or attack other computers. Some malicious code may also cause a DOS attack, reducing or completely eliminating a legitimate user’s access to systems or data.

(1) An infected e-mail message or attachment is the most common method by which viruses are spread. Automatic preview of messages (for example, in Microsoft® Outlook) has the same effect as opening the e-mail. Therefore, you should never configure your e-mail program to automatically preview e-mail messages. Instead, you should make a conscious decision on which e-mail messages to open. Always save e-mail attachments to your hard drive and scan them for viruses before opening them.

(2) Scan all removable media for malicious code before opening any of the files on a GC, regardless of whether or not the system is connected to an Army in Europe network.

(3) Virus-hoax warnings are also becoming more common. Most e-mail messages that warn of a virus use fake technical or emotional language to get the user’s attention. They include “urgent” requests to forward warnings to as many people as possible to protect everyone from a “devastating” virus. These messages are hoaxes and may even carry a virus themselves. Delete this type of e-mail and report it to your IASO. Forwarding it to other users accomplishes the sender’s goal of transmitting the message—and the virus—to as many users as possible. Even if there is no virus attached to the message, this kind of “chain mail” can overload e-mail systems and distract users from their official duties.

(4) A growing number of websites fall into the category of “malicious sites.” In particular, you should avoid clicking on links in e-mail messages that point to Internet addresses unfamiliar to you and “fake” links that might appear in interactive forms from untrustworthy sites. These links might actually be pointing to a site with a completely different Internet address than what you expect (that is, the real address will be hidden). These websites are often designed to exploit known operating system and other software vulnerabilities.

(5) The best antivirus course of action is to prevent your GC from being infected in the first place. Most importantly, you should ensure the antivirus software on your GC (and its supporting signature/definition file) is current. Your GC’s antivirus signature/definition files must be updated at least once a week. Antivirus software must also be updated on all Government-owned PDAs and other Government-owned PEDs. In most organizations, antivirus updates are automatically “pushed” to GCs, but you should still check your antivirus status periodically, including the setting to check “all files.” (Request assistance from your IMO or SA if needed.) Soldiers and DOD civilians may also install a DOD-approved antivirus program on their home computers free of charge. To do so, go to AKO to download the antivirus program of your choice.

(6) Deliberately introducing malicious code into any Government IS is a violation of a lawful general order under the Uniform Code of Military Justice (UCMJ), Article 92. Personnel not subject to the UCMJ may be subject to punitive or other administrative action under the United States Code, Federal regulations, or host-nation law. If you know of anyone violating this policy, you should report it immediately to your chain of command and to your IASO.

h. Defending Your Computer Against Hackers. Hackers may attempt to gain access to your system or the network. If they succeed, they may try to steal or manipulate information stored on or transmitted by your computer to other systems across the network. They may also attempt to use your system as a point from which to attack other systems (for example, to launch a DOS attack). As with defending your computer against viruses, the best way to defend your system and information against hackers is to prevent the intrusion in the first place.

(1) To protect your computer and the information stored on it, the best approach is to ensure that your computer's operating system and applications have the latest security-related patches installed.

(a) The intent of these patches is to "plug" security holes that were discovered in the software. If these holes are left open, hackers can develop ways to exploit the vulnerabilities, and your computer and possibly other computers to which your system is linked by a network connection will be at risk.

(b) Your IT support personnel are responsible for installing patches. When your unit purchases a new GC, when you use your GC preparing for or returning from TDY, or if your GC has been in storage or is disconnected for more than a week, you must take your GC to your IMO, SA, or IASO. The IMO, SA, or IASO will check the GC for viruses and confirm that is has all necessary patches, antivirus software, and definition files. Your IT support personnel will use the Army IA website at *https://informationassurance.us.army.mil/first-time/first-time.asp?/index.php* to quickly and safely prepare your computer for connection (or reconnection) to an Army in Europe network. They will also configure your system to automatically receive operating system, application, and antivirus updates from special-purpose servers after your system is connected to the network.

(2) As mentioned, hackers may also try to steal or modify information being transmitted across the network. All users must protect sensitive official information created and processed using automated systems such as e-mail and information posted on organizational intranet and extranet websites by using public key infrastructure (PKI). PKI enables digital signatures and encryption of sensitive information using certificates issued to individuals and stored on a hardware token such as your CAC. PKI-enabled CACs are issued to military, civilian, and contractor personnel and contain the following three certificates, which are digitally embedded in the card:

(a) Identity. This certificate permits access to your system along with some PKI-enabled websites and applications offering authentication mechanisms superior to the user-ID and password method. This certificate also enables users to digitally sign documents (for example Defense Travel System vouchers) to enable nonrepudiation (that is, the user cannot deny having signed the document).

(b) E-Mail Digital Signature. This certificate enables users to digitally sign e-mail messages to support strong authentication, prevent undetectable e-mail modification during transmission, and support nonrepudiation.

(c) E-Mail Encryption. This certificate protects the transmission of sensitive official e-mail messages from unauthorized or unintended disclosure. Since only the recipient's private key can decrypt encrypted e-mail, its content cannot be compromised.

(3) The following are examples of official information that must be *digitally signed* when sent by e-mail to any DOD, Army, or Army in Europe entity:

(a) Information relating to funds (for example, budgets, fiscal costs).

(b) Command directives that were initiated in the Defense Message System and transferred to e-mail.

(c) Command policy memorandums.

(d) Contract data.

(e) Unclassified administrative and logistical reports.

(4) The following are examples of official information that must be *digitally signed* and *encrypted* when sent by e-mail to any DOD, Army, or Army in Europe recipient:

(a) Sensitive operational information. This includes personally identifiable information (PII); unclassified tactical, administrative, and logistical information that supports the warfighter according to the USAREUR Critical Information List (for example, casualty reports, exercise deployment manning documents, information on installations and infrastructure, movement or transportation information, network data, unit status reports).

NOTE: The preferred means of sending unclassified information on operational matters is by classified e-mail message through the SIPRNET. Personnel should send this category of information through the NIPRNET using an unclassified e-mail account only if they do not have a classified e-mail account.

(b) Information marked FOUO (AR 25-55).

(c) Medical care, personnel management, and Privacy Act data (including social security numbers).

6. REPORTING COMPUTER SECURITY INCIDENTS

a. If you think you have observed a computer security incident or if you note some other security deficiency in your system or the network, you must report it to your IASO immediately. In general terms, a computer security incident is the act of violating an explicit or implied computer security policy. The following are examples of security incidents:

(1) Attempts to gain unauthorized access to a system or its data (for example, hacking).

(2) Attempts to defeat or circumvent computer-network or security controls (for example, Blue Coat, passwords).

(3) Writing or knowingly transmitting a virus, worm, or other form of malicious code.

(4) The events listed in AR 25-2, paragraph 4-21.

b. Specific actions to take when a system has been compromised are available on the Regional Computer Emergency Response Team-Europe (RCERT-E) website *https://www.rcerte.army.mil*.

c. If you suspect that your computer has been compromised, used for some type of crime, or used in an inappropriate way, you must ensure evidence is preserved by doing the following:

(1) Do not turn off your GC.

(2) Do not disconnect the GC from the network.

(3) Call your IMO, SA, or IASO. If they are unavailable, call the RCERT-E hotline (DSN 380-5232).

(4) Turn off the monitor and place a "HANDS OFF" notice on it, instructing everyone not to touch the computer.

(5) Control physical access to the computer. Ensure that no one tries to determine what happened on the computer before any investigative agencies have examined it.

7. PROTECTING DATA AT REST

a. Unclassified sensitive data or PII stored on desktops, laptops, portable notebooks, tablet PCs, external media, and similar systems are highly susceptible to theft and loss. These devices are commonly referred to as mobile computing devices (MCDs) or portable removable storage media (RSM) and are identified as especially high-risk when authorized for use in remote computing. "Sensitive information" is all unclassified Army information not specifically identified as public-releasable or -accessible.

b. Technology exists to prevent the unauthorized access to information stored on MCDs and RSM in case a device is lost. Immediate implementation of protective measures for MCDs and RSM is necessary to protect DAR and counter the effects of compromised information.

c. ISs processing Army information in mobile-computing environments must provide an encryption capability to protect DAR and in transit. This will help deter the ability of attackers to access files.

d. Only products offered through the U.S. Army Computer Hardware, Enterprise Software and Solutions (CHESS), may be used for encryption. The only authorized DAR-encryption solution for desktops, MCDs, and portable RSM is the Mobile Armor Data Protection Suite of encryption products (DataArmor, FileArmor, PolicyServer) and Microsoft XP Encrypting File System (EFS).

(1) Microsoft XP EFS is a file and folder product resident in the Microsoft Windows XP Service Pack 2. Because the Army intends to fully leverage its investment in the Microsoft Enterprise License Agreement, the existing EFS will continue as an authorized DAR tool.

(2) The Vista operating system provides further DAR capabilities (BitLocker), which in turn will become an authorized DAR tool once the Army migrates to the Vista operating system.

e. Stand-alone portable RSM devices that cannot be encrypted or store encrypted data are prohibited from being used to transmit or store sensitive data or PII.

f. Any DAR solution implemented before 27 October 2006 will be exempt until the license or maintenance agreements expire. No additional licenses are authorized to be purchased. On expiration of the license or maintenance agreement, the only products authorized for use in the Army will be the Mobile Armor Data Protection Suite of encryption products, Microsoft XP EFS, and Vista BitLocker (when Vista is implemented).

g. All MCD and RSM devices authorized for removal from a facility will be appropriately marked according to locally established procedures to indicate DAR compliance. All MCDs and RSM must implement DAR protection, regardless of their operating systems.

h. The MCD computer must be a domain-joined computer in a Windows 2000 or higher domain. If you use your CAC to log onto your computer, your computer is "domain-joined."

i. In all situations, users will take the "least risk" approach when transporting information on MCDs as follows:

(1) Never travel with information if an alternative, secure-transmission capability exists or a secure site or repository is available to store the information before or during travel.

(2) Use AKO as a repository for information-sharing.

(3) Use your CAC and PKI to provide secure transmission and nonrepudiation of e-mail.

(4) Travel with only the information absolutely necessary for mission objectives.

8. ISUT

a. Now that you have studied this guide, you are ready to take the ISUT. To do so, log on to the AE-ITT website at *https://itt.eur.army.mil*. Once you have taken and passed the test, you will receive your login credentials. Your authorization will be valid for 1 year. If you still need login credentials after 1 year, you will have to take the ISUT again.

b. Before you receive a login name and password for your GC, your IMO, SA, or IASO will require you to read and sign the Acceptable-Use Policy Agreement. Your signature acknowledges your understanding of the contents of this pamphlet and of the acceptable-use policy, and indicates your commitment to support DOD, Army, and Army in Europe policy on the use of GCs. Your signature also makes you accountable for every action that is generated using your GC user account. If you refuse to sign the Acceptable-Use Policy Agreement, you will not be given an account for any system or network in the Army in Europe. Computer users will read and sign a new Acceptable-Use Policy Agreement every time they take the ISUT.

9. CONCLUSION

As a GC user, you play a key role in protecting the confidentiality, integrity, and availability of information in the Army in Europe. By taking the basic steps outlined in this pamphlet, you will help ensure that your GC and all networks to which it is connected are secure. You will be protecting not only yourself, you will be protecting the entire Army in Europe.

GLOSSARY

SECTION I
ABBREVIATIONS

AE	Army in Europe
AE-ITT	Army in Europe Information Technology Training
AKO	Army Knowledge Online
AOL	America Online
AR	Army regulation
CAC	common access card
CHESS	Computer Hardware, Enterprise Software and Solutions
CIO	chief information officer
DA	Department of the Army
DAA	designated approving authority
DAR	data at rest
DOD	Department of Defense
DOS	denial of service
DSN	Defense Switched Network
DTG	date-time group
EFS	Encrypting File System
FOUO	For Official Use Only
GC	Government computer
HQ USAREUR/7A	Headquarters, United States Army Europe and Seventh Army
IA	information assurance
IAM	information assurance manager
IAPM	information assurance program manager
IASO	information assurance security officer
ID	identification
IMO	information management officer
IS	information system
ISP	Internet service provider
ISUT	Information Systems User Test
IT	information technology
JER	Joint Ethics Regulation
MCD	mobile computing device
MPEG	Moving Picture Experts Group
MSN	Microsoft Network
NATO	North Atlantic Treaty Organization
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
PDA	personal digital assistant
PDS	protected distribution system
PED	personal electronic device
PII	personally identifiable information
PIN	personal identification number
PKI	public key infrastructure
RCERT-E	Regional Computer Emergency Response Team-Europe
RSM	removable storage media
SA	system administrator

SIPRNET	Secret Internet Protocol Router Network
TDY	temporary duty
UCMJ	Uniform Code of Military Justice
URL	uniform resource locator
U.S.	United States
USAREUR	United States Army Europe
USB	universal serial bus
USEUCOM	United States European Command

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 automated information systems, computers, and telecommunications. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, distribute, process, store, or control data or information.

NIPRNET
The network of Internet protocol routers owned by DOD and created by the Defense Information Systems Agency. The NIPRNET is used to exchange unclassified but sensitive information between internal users and to provide users access to the Internet.

personally identifiable information (PII)
Information that can be used to distinguish or trace an individual's identity, including but not limited to the individual's name, birth date, home address, social security number, pay information, and Family information.

SIPRNET
The network of interconnected computer networks used by DOD to transmit classified information (up to and including information classified Secret) in a secure environment.