Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command,
Europe Region
Sembach, Germany

Army in Europe
Pamphlet 25-25*

17 October 2013

Information Management

Army in Europe Information Technology Users Guide

***This pamphlet supersedes AE Pamphlet 25-25, 29 September 2011.**

For the Commander:

JAMES B. MINGO
Colonel, GS
Chief of Staff

Official:

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This pamphlet provides guidance on the authorized use of information technology in the Army in Europe. Specifically, it emphasizes the secure and responsible use of Government computers in a manner that ensures the protection of Army in Europe systems against threats to the confidentiality, integrity, and availability of the information stored, processed, or transmitted by those systems.

Summary of Change. This revision—

● Incorporates current security requirements and updated Department of the Army (DA), Defense Information Systems Agency, Army CIO/G-6, and Army in Europe policy.

● Incorporates additional tokens as part of the credential requirements for the SIPRNET and the NIPRNET (para 5h).

● Updates the Army in Europe network policy violation-escalation process (para 5k).

● Updates network user account requirements (para 8).

● Updates training requirements (para 8b(2)).

● Makes administrative changes throughout.

Applicability. This pamphlet applies to all DOD military, civilian, and contractor personnel (including non-U.S. personnel) in the Army in Europe. This includes contractors who are explicitly authorized by contract to connect their own computers to Army in Europe networks to conduct Government business.

Suggested Improvements. The proponent of this pamphlet is the Information Assurance Program Management Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR (mil 537-6203). Users may send suggested improvements to this pamphlet by e-mail to the USAREUR G6 (AEIM-I) at usarmy.wiesbaden.usareur.list.dl-g6-iapm@mail.mil.

CONTENTS

---

1. PURPOSE

The purpose of this pamphlet is to outline the roles and responsibilities of Government computer (GC) and network users. This pamphlet also describes the administrative and judicial sanctions that may be enacted on users who knowingly, willingly, or by negligence compromise, damage, or place at risk DOD information systems (ISs) by not following DOD, Department of the Army (DA), or Army in Europe policy and procedures.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. THE THREAT

a. U.S. warfighting capability depends on the confidentiality, integrity, and availability of information. An effective protection of information and ISs gives Soldiers an advantage in the information superiority battlefield by enabling them to make timely and sound operational decisions. Our ISs, however, are continuously being attacked, externally and internally. The external threats range

from hackers and virus distributors to state-sponsored, sophisticated cyber terrorists. The internal threats include intentional and unintentional actions by members of our own workforce.

b. GCs store, process, and transmit unclassified data and sensitive information and are interconnected through a data network known as the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET). Your GC can be reached by other systems on the NIPRNET and simultaneously connect to resources on the Internet. Although the Secret Internet Protocol Router Network (SIPRNET) 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. Whether you use a NIPRNET or SIPRNET device in your work environment, your computer is a gateway to a vast amount of information, much of which is sensitive or classified and may not be released to the public.

c. The best defense against threats to our information and ISs is through the application of sound information assurance (IA) guidance, which relies on a trained, aware, and vigilant workforce. Although commanders are ultimately responsible for the confidentiality, integrity, and availability of USAREUR networks, they need the help of every DOD GC user. As a GC user in the European theater, you play a key role in protecting data and ISs.

5. MINIMIZING THE RISK

a. Consent to Auditing and Monitoring. All DOD employees in the Army in Europe who use Government communication systems must understand that they consent to the auditing and monitoring of actions they perform on these systems, as outlined on the GC's logon warning banner. Clicking "OK" on the banner indicates that you understand that your activity is monitored and that you waive any reasonable expectations to privacy. When you log on to a GC, you agree to these terms. Authorized monitoring and account-activity logging enables account activity to be reconstructed, if necessary, which will reveal any user actions that violate policy or bypass security controls. Violating or bypassing established security controls will lead to the seizure of a user's GC to initiate further investigation. GCs may not be used for unlawful activities. Attempts to conduct such activities on Government systems will be considered network violations and will result in the user's account being disabled or other punitive actions. Law-enforcement and counterintelligence agencies may be notified to investigate any unlawful use of GCs, as authorized by pertinent laws.

(1) The measures implemented to safeguard Army in Europe ISs and data are based on lawful DOD policies. However, you may seek legal counsel if you have concerns related to information protection, privileges, or confidentiality.

(2) Users must know which of the systems and data they access are protected and confidential in nature. Security managers and data owners define the sensitivity of the information on a system. Although users may suggest that a system or data be treated as protected at a certain level, they may not arbitrarily label a system or information. Any such assertion will be unbinding, unless specified in existing standards or DOD policy.

(3) The U.S. Government reserves the right to label all DOD systems and data. In addition, the U.S. Government will employ reasonable measures to protect the content of captured or seized systems and data stored on these systems.

(4) Audit data on a GC is collected and retained for a period of 1 year to support technical analyses relating to misuse, penetration reconstruction, or other investigations.

b. Authorized Use. Your GC and all output generated by it (for example, printed documents) are the property of the U.S. Government or, in some cases, of a Government contractor as part of a contract requirement. GCs may be used only by Government employees and Government contractors for official and authorized purposes. Users may access only data, systems, and programs they are specifically authorized to use. They will not attempt to gain unauthorized access to systems or data.

(1) All DOD network users are assigned an information technology (IT) level. Most users are in positions designated as IT level III. Users who are granted elevated access to Army in Europe GCs and networks are in positions designated as IT level I or II and required to undergo periodic background investigations.

(2) The use of the NIPRNET for personal purposes is authorized in support of Internet-based capabilities (IBCs) provided the use meets all of the following requirements:

(a) Conforms to DOD, DA, and Army in Europe policies.

(b) Does not adversely affect the performance of duties.

(c) Serves a legitimate public interest such as activities related to morale, welfare, and recreation or self-improvement activities directly related to the scope of duties performed.

(d) Does not overburden the Army in Europe communication system, the primary purpose of which is to support mission requirements.

(3) Commercial webmail services (for example, America Online, Gmail, Hotmail, Yahoo) are prohibited for conducting official Army business.

(4) Sites with questionable or prohibited content are inaccessible from Army in Europe networks. Users are required to submit a Remedy trouble ticket either by telephone (119) or through the Internet (*https://119.eur.army.mil*) if they need access to an inaccessible website to perform their duties. Users may contact the local network control center (NCC) for information on how to gain access to mission-essential websites or if they believe that a site has been incorrectly categorized. If a blocked site was not approved by the NCC and further justification must be submitted to obtain approval, contact your information assurance manager (IAM) for additional assistance.

(5) The following are some of the activities that are prohibited on the Army in Europe NIPRNET:

(a) Using someone else's common access card (CAC).

(b) Providing unauthorized individuals access to a GC or Government data.

(c) Gaining unauthorized access to or from a GC in an attempt to compromise another system or disclose data.

(d) Storing, processing, displaying, or transmitting offensive or obscene content that is racial, sexually explicit, harassing, or hateful.

(e) Storing or processing copyrighted material, unless approval is obtained from the author or publisher. In addition, such material must be mission-related.

(f) Forwarding official e-mail to and from a non-Government e-mail service.

(g) Online gambling.

(h) Managing personal homepages, online games, or other unofficial business.

(i) Processing data that exceeds the classification level of the network being used (that is, processing classified information on unclassified systems).

(j) Processing information that is proprietary, contractor-excluded, or identified as needing restricted handling.

c. Special Considerations for Using the SIPRNET. The following are some of the considerations that must be kept in mind when using the Army in Europe SIPRNET:

(1) Unauthorized data transfers routinely occur on classified networks when removable media is used. To mitigate such activity, SIPRNET GCs have the "write" features disabled as part of the Army in Europe group-policy configuration. Users are not authorized to write to removable media storage devices (RMSDs) on SIPRNET GCs. SIPRNET users who need "write" privileges must follow the procedures in USAREUR TASKORD 11-0101 to request this capability.

(2) Users may not enter information into a system if the information has a higher classification than that for which the system is accredited.

(3) Restrictions apply when processing information that is proprietary, contractor-excluded, or identified as needing restricted handling.

(4) Only U.S. personnel with proper security clearances coupled with the need to know are allowed access to GCs connected to SIPRNET.

(5) Personnel without a security clearance will not have access to areas where SIPRNET equipment is located. If physical access to such an area is required, such personnel will contact their security managers for further guidance.

(6) Users must not bring any wireless electronic devices into a classified workarea. They should contact the responsible security manager for more information.

(7) All users must use a SIPRNET token and an associated personal identification number (PIN) to access the SIPRNET and public key infrastructure (PKI)-enabled e-mail.

d. Authorized Software and Hardware. Software and hardware installed on a GC must be properly licensed. Users must coordinate the acquisition and use of software and hardware with the responsible information management officer (IMO) or IAM. Any changes to a GC's configuration, including changes to connected devices, must be formally requested from and approved by the responsible IMO or IAM. Users must not modify or tamper with the software or hardware of their GC or move a GC to another location unless the responsible IMO, system administrator (SA), or IAM authorizes them to do so.

(1) Any software that is purchased to support an organization's mission and that is not part of the Army Gold Master must be in the DOD Unified Capabilities Certification Office Approved Products List Integrated Tracking System, which can be found on the Defense Information Systems Agency

website (*https://aplits.disa.mil/CAS/login*). You may also contact your IAM or IMO for additional guidance before purchasing the product.

(2) Prohibited software that may not be installed on GCs includes peer-to-peer file-sharing, music- and video-sharing, hacker tools, malicious-code-development software, and network-monitoring (that is, packet sniffing) and keystroke-monitoring tools. Other prohibited software includes unlicensed ("pirated") copies of computer programs, webpage-altering software, games (including "America's Army"), and personal firewalls. Additionally, you must not obtain, install, copy, store, or use software if doing so would violate the vendor's license agreement. You must not download or install freeware or shareware on a GC. Contact your IAM for exception-to-policy procedures or other information.

(3) Devices connected to the NIPRNET automatically have their wireless functionality disabled as part of the group-policy configuration. This applies to GCs and all Government-approved Bluetooth wireless devices. Users are not authorized to reactivate the wireless capability on their own. Contact your IMO or IAM if your GC's wireless functionality needs to be activated for mission-related reasons such as TDY travel. After your return from TDY, your IMO or IAM will ensure the wireless capability is disabled.

(4) Never connect a modem, iPod, commercial cellular phone, or any unauthorized device to a GC. Contact your IAM or IMO for guidance and proper authorization.

(5) Do not connect your GC to a commercial Internet service provider (ISP) while the GC remains connected to a Government network.

(6) You may be authorized to connect to the Army in Europe NIPRNET through a Virtual Private Network (VPN) using a commercial ISP. If so, a VPN user account and a GC with installed approved VPN client software are required.

e. Responsible Use of IBCs and Social Networking Systems (SNSs). The use of IBCs and SNSs provides an attractive way to communicate and share information with computer users who have similar interests. When participating in these new capabilities, you should be aware of the risks.

(1) When opening an IBC or SNS portal on your GC, you may be exposing your GC to—

(a) Malware.

(b) Session hijacking.

(c) Address and identity spoofing.

(d) Cookies, which can be placed on your system and redirect your GC to questionable sites.

(2) Visiting IBC or SNS sites raises serious security concerns, as these sites are accessible to adversaries who try to compile information that is of use to them. Therefore, when opening SNS sites, never disclose information that is—

(a) Classified or For Official Use Only (FOUO).

(b) Sensitive, such as casualty information being disclosed before the next of kin has been formally notified by the military service.

(c) Protected by the Privacy Act of 1974.

(d) Personally identifiable.

(e) Alluding to ongoing investigations.

(f) Considered mission-essential.

(g) Found on the critical information list.

(h) Related to Government acquisitions or contracts.

(i) Likely to have an adverse effect on the interests of USAREUR, DA, DOD, or the U.S. Government or its allies if disclosed.

NOTE: Your public affairs office can provide additional guidance on SNSs.

(3) During periods of heightened network activity, the Army in Europe may minimize non-mission-essential activity on our networks. When such an order is in effect, the personal use of GCs on Army in Europe networks is prohibited for the duration of the order, except for e-mail messages between deployed Soldiers and their Families.

f. Taking Care of Your Computer. As a GC user, you must—

(1) Safeguard your GC against theft and compromise.

(2) Treat your GC with care to ensure proper functioning.

(a) Shut down your GC at the end of the duty day and before going on leave or TDY, unless your IMO or IAM tells you otherwise. Do not change your GC's power settings; doing so may adversely affect the energy-saving mode of your system. Contact your IMO if you have questions concerning the energy-saving mode of your GC.

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

(c) Never disconnect your GC from the network unless specifically directed to do so by your IMO, SA, IAM, or information assurance support officer (IASO).

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

(3) Laptops taken by the user on missions away from the office are particularly susceptible to theft. With the right tools, anyone who has physical access to your system can take control of your GC and steal, delete, or manipulate your data. For more information, contact your security manager.

(4) All GCs used outside of the office (for example, while travelling or working from home) must be in compliance with DA and Army in Europe data at rest (DAR) encryption requirements, as outlined in paragraph 7b.

g. Handling Classified Material. Special care must be taken when handling classified material.

(1) All media and documents must be properly labeled at the highest classification of the information they contain. Official labels are Unclassified, Confidential, Secret, and Top Secret. This is imperative when working in an area where both NIPRNET and SIPRNET access is available.

NOTE: GCs must be conspicuously labeled according to the classification of the data being processed on them (for example, Unclassified for NIPRNET and Confidential or Secret for SIPRNET).

(2) In cases where the designated approving authority (DAA) has approved removable-media write privileges on the SIPRNET, any writable RMSD inserted into or attached to a system labeled Secret automatically becomes Secret and must be handled accordingly, regardless of the direction of data flow and the actual classification of the data involved. Classified computers, documents, and other media must not be removed from a classified workarea without the security manager's approval.

(3) Your security manager will issue courier orders to individuals who need to transport classified material. When doing so, the security manager will determine if courier orders are necessary, verify that the individual has a clearance that is appropriate to the level of material to be transported, and instruct the courier on the proper packing of classified material.

(4) If you work in an area explicitly and properly approved as an open-storage area, you must follow the security procedures established for that area.

(5) When handling classified material in an area that is not approved for open storage of classified material, you must lock all classified devices and all classified material (printed and electronic) in a General Services Administration approved security container and follow the established security procedures when departing the workarea.

h. Protecting Your Credential. You are required to use your token (CAC for the NIPRNET or alternate smart card logon (ASCL) token for the SIPRNET) and the applicable PIN to access your GC on the NIPRNET or SIPRNET. No exception is granted to use a username and password combination to log on to a GC.

(1) Protect your log-on credentials. Your log-on credentials grant access to Army in Europe networks and the Internet. Protecting your credentials is imperative to prevent others from gaining access to the resources you were entrusted with. You are responsible for any activity that takes place on a GC under your credentials, including any e-mail messages that originate from your account. Use the following guidelines to protect your network log-on credentials (CAC or ASCL token and PIN), which were established to access Government resources:

(a) Do not share them.

(b) Do not write them down or post them in places accessible to others.

(c) Do not store them online.

(d) Do not store them on electronic devices or media accessible to others.

(e) If you suspect that your PIN has been compromised, contact your IMO or IAM immediately. Your account will be disabled until your PIN has been reset.

(2) You will be prompted to change your password every 90 days for VPN accounts. In rare situations when the username is used, the following is required:

(a) General-user passwords must have at least 14 characters and include at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters.

(b) Privileged users, such as system and domain administrators, are required to use an ASCL token to perform required duties.

(c) In limited cases where an ASCL is not used or not available, privileged user-names and passwords are required. Privileged user passwords must have at least 15 characters and include at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters.

(d) Passwords must not form a word or repeat any of your last 10 passwords. Your system will not accept passwords that do not meet these requirements.

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

(4) If you have a SIPRNET account, you must log on to the SIPRNET within 35 days after your account was established and at least once every 35 days afterward to prevent the account from being disabled. The account will be deleted after 60 days if no action is taken on the part of the user.

NOTE: Your CAC is the property of the U.S. Government and must be in your custody at all times. Misplaced or lost CACs can result in unauthorized access to DOD information systems and U.S. military bases.

i. Defending your GC against Viruses and Hackers. Viruses and worms (or malware) are programs that may corrupt computer applications, computer data, or both. Malware may provide hackers access to your computer and allow them to attack other systems from your GC, causing a disruption or disabling legitimate users' access to computer or network resources. To protect your GC and the information stored on it, your GC is equipped with DOD-approved and continuously updated antivirus software. In addition, your GC's operating system and software are continually being updated with the latest security patches. To minimize the possibility of infecting your GC with malware, you should—

(1) Ask your IMO if the use of a particular removable medium is authorized before connecting it to your GC.

(2) Not open suspicious e-mail messages.

(3) Contact your IMO, IAM, or IASO if you believe you have received an e-mail message containing malware.

(4) Not forward any e-mail messages from unknown sources that claim to be "urgent" or state that they must be distributed to as many people as possible. These e-mail messages are considered hoaxes. Forwarding "chain mail" is prohibited.

(5) Be suspicious of links embedded in e-mail messages you receive. Do not click on them. These links often point to questionable sites or redirect you to sites you normally would not want to visit. In addition, these websites are often designed to exploit known operating-system and other software vulnerabilities.

(6) Ensure your GC remains connected to an Army in Europe network so its antivirus software and virus definitions can be updated and security patches can be applied.

(7) When you return from TDY with a Government laptop that you used during the trip, contact your IMO before reconnecting the laptop to the Army in Europe network. The IMO will determine whether or not your laptop is safe to be connected to the network. Depending on the length of the TDY, your laptop may have to be scanned and updated or reconnected to the domain.

(8) Consider installing the DOD-approved antivirus software on your personal home systems to prevent malware infection and distribution. The Army Home Use program makes it easy for Army Soldiers and Government Civilians to secure their home computers by giving them free access to both Symantec and McAfee antivirus software and firewalls at *https://www.acert.1stiocmd.army.mil/Antivirus/*.

(9) Deliberately introducing malicious code into a GC is a violation punishable under the Uniform Code of Military Justice (UCMJ) and a violation of Army in Europe network policy. Personnel not subject to the UCMJ may be subject to punitive or administrative actions under other applicable laws. All users who violate network policy will immediately lose their access to the network. AE Regulation 25-2 prescribes procedures for users to request that their network access be restored.

j. Individual Accountability. Cybersecurity is everyone's business. You are the key to protecting U.S. Government and U.S. Army information and information systems. The following are unauthorized activities on Army in Europe networks:

(1) Connecting personally owned electronic devices to Army in Europe networks or GCs. This includes but is not limited to personal computers (PCs), mobile computing devices (MCDs), universal serial bus (USB) memory devices, cell phones, cameras, and audio devices.

(2) Accessing or using Internet content such as gambling, auctions, malware, pornography, and personal dating services.

(3) Accessing information without proper authorization or a valid need to know including viewing classified data on third-party Internet sites.

(4) Physically connecting classified systems to unclassified domains or networks.

(5) Disabling, modifying, or bypassing protective software or data logs.

(6) Using privileged-level access for non-mission or user-level tasks such as browsing the Internet.

NOTE: The preceding list is not intended to be all inclusive. Consult with your IASO, IMO, or IAM if you are unsure of actions taken on your GC. Asking may prevent a violation or serious incident, unnecessary work, and a loss of network access and workhours.

k. Sanctions. Any military or civilian personnel who knowingly, willfully, or by negligence compromise, damage, or place at risk any Army in Europe IS by not ensuring the implementation of DOD system security guidelines in accordance with this pamphlet, DOD 8500-series directives and

instructions, DOD Regulation 5200.1-R, AE Regulation 25-2, and supplemental USAREUR policies and procedures are subject to administrative or judicial sanctions, or both.

(1) Sanctions for military personnel may range from an oral or written warning or reprimand to administrative measures or nonjudicial or judicial punishments authorized by the UCMJ.

(2) Sanctions for civilian personnel may include an oral or written warning or reprimand, an adverse performance evaluation, or suspension from work. Sanctions may also include prosecution in U.S. district courts or other courts and sentences pursuant to such prosecution.

(3) DOD contractors are responsible for ensuring that employees perform under the terms of the contract and applicable directives, laws, and regulations and must maintain employee discipline. Criminal jurisdiction in the United States could be asserted by Federal, state, or local authorities, and by foreign state authorities for certain offenses committed abroad.

(4) According to AE Regulation 25-2, all network users who commit network violations will have their accounts disabled. AE Regulation 25-2 prescribes procedures for users to request that their network access be restored.

NOTE: Commanders may take nonpunitive actions such as suspending a user's access to classified or unclassified networks or requiring a user to repeat required user training. Commanders may refer to the "Commander's Quick Reference Guide to Defending Cyberspace" (AE Reg 25-2, app F).

l. PKI. The DOD PKI, which is used on the NIPRNET and the SIPRNET, adds a layer of protection by using digital signatures and encryption capabilities. Many DOD portals use PKI for access and rely on the certificates stored on a hardware token or CAC.

(1) Your CAC includes the following three certificates:

(a) Identity. This certificate permits access to your system along with PKI-enabled websites and PKI-aware applications that offer authentication mechanisms. It also enables users to digitally sign documents, which eliminates the need for a standard (or "analog") signature.

(b) E-Mail Digital Signature. This certificate is used to digitally sign e-mail messages, which prevents undetectable modifications to the messages during transmission. It also supports nonrepudiation, which prevents the sender of an e-mail message from denying authorship of the message.

(c) E-Mail Encryption. This certificate protects the contents of an e-mail message from unauthorized or unintended disclosure by ensuring that only the intended recipient will be able to open the message.

(2) All official e-mail must be digitally signed.

(3) Some official e-mail messages must be both digitally signed and encrypted when sent by e-mail to any DOD, DA, or Army in Europe recipient. The following are examples of information that must be both digitally signed and encrypted when sent by e-mail.

(a) Sensitive operational information. This includes personally identifiable information (PII); unclassified tactical, administrative, and logistic information that supports Soldiers, such as casualty

reports and exercise deployment manning documents; information about installations and infrastructure; movement and transportation information; network data; and unit status reports. The SIPRNET is the preferred means of sending unclassified messages that include information concerning operational matters.

(b) Information marked For Official Use Only or FOUO.

(c) Information concerning medical care, the Health Insurance Portability and Accountability Act, personnel management, and information protected by the Privacy Act (including PII).

NOTE: No classified information may be sent by NIPRNET e-mail, even when digitally signed and encrypted.

6. CYBER INCIDENTS

a. Types of Incidents. AR 25-2, section VIII, paragraph 4-21, states that incidents may result from accidental or deliberate actions on the part of a user or from external influences. Evidence or suspicion of an incident, intrusion, or criminal activity will be treated with care, and the IS will be maintained without change, pending coordination with IA specialists, the Army Computer Emergency Response Team, the Regional Computer Emergency Response Team–Europe (RCERT-E), and law-enforcement or counterintelligence personnel. All personnel will report potential or malicious events including but not limited to the following:

(1) Incidents of known or suspected intrusion or access by an unauthorized individual, such as—

(a) Logs revealing unauthorized access to an IS.

(b) Unexplained modifications of files, software, or programs.

(c) The presence of suspicious files, shortcuts, or programs.

(d) Unexplained or erratic IS system responses.

(e) Webpage defacement.

(2) Authorized users attempting to circumvent security procedures or elevate access privileges by—

(a) Using unauthorized proxies to circumvent protective measures.

(b) Introducing unauthorized hardware or devices to the network (for example, digital cameras, flash-based removable media, gaming consoles, Global Positioning System devices, MP3 players, PCs, personal digital assistants, personally owned external hard drives, smartphones, wireless access points).

(c) Using unauthorized software to elevate system privileges (for example, key generators, key loggers, password crackers).

(d) Using peer-to-peer software to download or upload unauthorized files.

(3) Indications of malicious logic infection, such as—

(a) Virus, worm, or Trojan activity.

(b) Antivirus alerts of potential infections.

(c) Suspicious connections or beaconing to unknown destinations.

(d) An unexplained change of background or the presence of suspicious files, shortcuts, or programs.

(4) The receipt of suspicious e-mail messages containing suspicious attachments, files, or links, such as—

(a) Suspected social-engineering messages targeting DOD operations or events.

(b) Unsolicited messages that request personal or financial information from the recipient or offer products that are "too good to be true" (phishing messages).

(c) Spam messages that contain attachments or links to content of a questionable nature (for example, banking scams, e-greeting cards, geopolitical information, pharmaceuticals, pornography).

(5) Serious incidents or network policy violations of published Best Business Practice procedures, such as—

(a) Classified information identified in transit.

(b) Third-party notification of a network-security violation or cross-domain activity.

(c) Disclosure of PII due to a system or network compromise.

b. Reporting Cyber Incidents. In accordance with AR 25-2, section VIII, paragraph 4-22, an individual who suspects or observes an unusual event or obvious cyber incident on an IS will immediately cease all activities and notify the IAM, SA, or network administrator (NA).

c. Handling Cyber Incidents. IAMs, SAs, and NAs who observe, suspect, or receive information about a cyber incident will do the following:

(1) Logically isolate the system and prohibit any additional activities on or to the system.

(2) Ensure that the state of the system suspected of compromise is secured by—

(a) Disconnecting the system from the network by unplugging the network cable.

(b) Leaving the GC turned on and turning off the monitor placing a "Hands Off" notice on it.

(c) Not attempting to investigate or access the system unless directed by the RCERT-E.

(d) Not altering or changing the system files on the suspected system.

(e) Not attempting to contact the source directly.

(f) Not allowing any suspected individuals access to the system.

(g) Ensuring the state of the system is not altered before conducting incident-response actions as directed by the RCERT-E.

(3) After securing the system, complete the RCERT-E Cyber Event Notification Form found on the RCERT-E website at *https://www.rcerte.army.mil/* under the "Report an Incident" tab.

7. PROTECTING YOUR DATA

a. Sensitive Information. Sensitive information is all unclassified Army information not specifically identified as public-releasable or -accessible. Sensitive information and PII must be guarded from unauthorized access and compromise. This information is commonly stored and processed on devices referred to as MCDs such as—

(1) Laptops and notebooks.

(2) Smartphones.

(3) Tablet computers.

b. DAR. Microsoft Windows BitLocker is the approved DAR solution for the Army in Europe. All sensitive information and PII stored or processed on MCDs or stored or transported on an RMSD must be protected. Using a proper DAR solution prevents unintended users from accessing information stored on approved MCDs and RMSDs.

(1) PII and sensitive information stored on your GC is automatically protected with DAR.

(2) Data placed on other devices and media must be explicitly encrypted. Contact your IMO for instructions on how to encrypt files.

c. Transporting Sensitive Information. When transporting PII or sensitive information, adhere to the following best practices:

(1) Confirm that your GC has been configured with BitLocker (b above).

(2) Do not travel with PII or other sensitive information if alternative secure transmission capabilities exist.

(3) Use a shared drive or network drive to store important information before traveling. This will help ensure you can recover your sensitive information from the backup in case your MCD or RMSD is lost, compromised, or malfunctions.

(4) Use the AKO portal for information-sharing and storage, if feasible. Make sure you grant access to your AKO-stored files only to personnel who should have access to them.

(5) Travel with only the information that is necessary to support your mission. This will minimize damage if your MCD or RMSD is lost, compromised, or malfunctions during your trip.

8. ACQUIRING A COMPUTER ACCOUNT

The process below outlines the steps that must be taken before a computer account can be granted. Your sponsor or IMO will provide you with a step-by-step checklist that will further explain what you need to do before receiving a computer account. Initial access to training websites can be obtained by using the

DOD Guest account feature until all requirements are met to have a computer-user account created or enabled.

a. Ensure you have an active AKO account if you are authorized to have one. Incoming DOD civilian employees are authorized to self-register for an account. Local national employees and DOD contractors must be sponsored by authorized personnel before an AKO account can be created for them. Refer to the guidance posted on the AKO portal at *http://www.us.army.mil/* for further instruction. Having an AKO account alone, however, does not constitute eligibility for a computer-user account.

b. To obtain a user and e-mail account, all computer users are required to—

(1) Create an Army Training and Certification Tracking System (ATCTS) account at *https://atc.us.army.mil/* and an Army in Europe Information Technology Training account at *https://itt.eur.army.mil/*.

(2) Create an Information Assurance Training Center account at *https://ia.signal.army.mil/* and complete the DOD Cybersecurity Awareness Challenge (formally known as IA Awareness Training and Exam). Results will automatically be uploaded in the individual's ATCTS account.

(3) Read and digitally sign the Acceptable Use Policy (AUP) agreement (*https://ia.signal.army.mil/*). The signed AUP agreement will automatically be uploaded in your ATCTS account.

NOTE: By signing the AUP agreement, you acknowledge that you understand and accept its content. Your signature signifies your commitment to adhere to the DOD, DA, and Army in Europe GC use policy. Your signature also confirms you understand that you will be held responsible for all actions conducted on a GC and the network that were generated from your user account. If you refuse to sign the AUP agreement, you will not be given an account for any system or network in the Army in Europe. Users will read and sign a new AUP agreement every time they take the IA Awareness Training.

(4) Complete DD Form 2875, which is the source document for validating the personnel security designation for system access, and upload the completed form in your ATCTS account.

(5) Ensure ATCTS profiles are updated, verified, and correct.

NOTE: New users may require IMO assistance to perform the actions above.

9. CONCLUSION

As a GC user, you play a vital role in protecting the confidentiality, integrity, and availability of Government information. By following the basic steps outlined in this pamphlet, you will help ensure that your GC, the Army in Europe network, and the information you process are protected. By following these procedures, you will be protecting not only your own GC system and the information you process, but also the missions of the Army in Europe, DA, and DOD.

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)

DOD 5500.7-R, Joint Ethics Regulation (JER)

DOD 8570.01-M, Information Assurance Workforce Improvement Program

AR 25-1, Army Information Technology

AR 25-2, Information Assurance

AR 25-55, The Department of the Army Freedom of Information Act Program

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

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

AE Regulation 25-2, Army in Europe Information Assurance

USAREUR TASKORD 11-0101, Protecting Classified Information on DOD SIPRNET

SECTION II
FORMS

DD Form 2875, System Authorization Access Request (SAAR)

GLOSSARY

SECTION I
ABBREVIATIONS

AE	Army in Europe
AKO	Army Knowledge Online
AR	Army regulation
ASCL	alternate smart card logon
ATCTS	Army Training and Certification Tracking System
AUP	Acceptable Use Policy
CAC	common access card
CIO/G-6	Army Chief Information Officer, G-6
DA	Department of the Army
DAA	designated approving authority
DAR	data at rest
DOD	Department of Defense
FOUO	For Official Use Only
GC	Government computer
HQ USAREUR	Headquarters, United States Army Europe
IA	information assurance
IAM	information assurance manager
IASO	information assurance support officer
IBC	Internet-based capability
IMO	information management officer
IS	information system
ISP	Internet service provider
IT	information technology
MCD	mobile computing device
NA	network administrator
NATO	North Atlantic Treaty Organization
NCC	network control center
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
PC	personal computer
PII	personally identifiable information
PIN	personal identification number
PKI	public key infrastructure
RCERT-E	Regional Computer Emergency Response Team–Europe
RMSD	removable media storage device
SA	system administrator
SIPRNET	Secret Internet Protocol Router Network
SNS	social networking system
TASKORD	tasking order
TDY	temporary duty
UCMJ	Uniform Code of Military Justice
U.S.	United States
USAREUR	United States Army Europe
USAREUR G6	Deputy Chief of Staff, G6, United States Army Europe
USB	universal serial bus
VPN	Virtual Private Network

SECTION II
TERMS

accountability
An individual's responsibility for safeguarding and controlling information-technology and communications-security equipment, keying materiel, and information entrusted to him or her. If equipment is lost or if an audit of activities conducted on an information system used by the individual reveals misuse, that individual will be held responsible.

consent to monitoring
A computer user's agreement to the auditing and monitoring of the actions performed on a U.S. Government computer (GC). All DOD employees in the Army in Europe who use Government communication systems must understand that they consent to the auditing and monitoring of actions they perform on these systems, as outlined on the GC's log-on warning banner. Clicking "OK" on the warning banner indicates that the user understands that his or her activity may be monitored and that any reasonable expectations to privacy have been waived.

information assurance (IA)
The protection of systems and information in storage, processing, or transit from unauthorized access or modification; the denial of service to unauthorized users; and the provision of service to authorized users. IA also includes measures that are necessary to detect, document, and counter such threats as well as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA comprises the security discipline that encompasses communications security, information security, and the control of compromising emanations.

information system (IS) security incident
Any unexplained event that could result in the loss, corruption, or denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of a system. An IS security incident can also be an occurrence of classified or sensitive information being processed by an IS where a deviation from the requirements of the governing security regulations may exist; a suspected or confirmed compromise or unauthorized disclosure of the information; questionable data or information integrity (for example, unauthorized modification); unauthorized modification of data; or information not being available for a period of time. Also included are attempts to exploit any IS in a way that the actual or potential adverse effects may involve fraud, waste, or abuse; a compromise of information; a loss or damage of property or information; or a denial of service. IS security incidents include the penetration of computer systems, the exploitation of technical and administrative vulnerabilities, and the introduction of computer viruses or other forms of malicious code.

information technology (IT)
The study, design, development, implementation, and management of computer-based information systems, including software applications and computer hardware. IT comprises the use of computer systems and software to convert, store, protect, process, transmit, and securely retrieve information.

personally identifiable information
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.

Secret Internet Protocol Router Network (SIPRNET)
The network of interconnected computer networks that is used by DOD to transmit classified information in a secure environment and that has become the core of the Army's warfighting command-and-control capability. Although the SIPRNET uses the same communications procedures as the Internet, it has dedicated encrypted lines that are separate from all other communication systems.

Unclassified but Sensitive Internet Protocol Router Network
The network of Internet protocol routers that is used to exchange unclassified but sensitive information between DOD users and provide users access to the Internet. It is owned by DOD and maintained by the Defense Information Systems Agency.