Requirements for Obtaining an Unclassified US Army In Europe LandWarNet (LWN-U)

Computer User Account

1 **CAC –** Common Access Card. To log on to the network, users are required to have a CAC. If you do not have a CAC click here to find out how to get one.

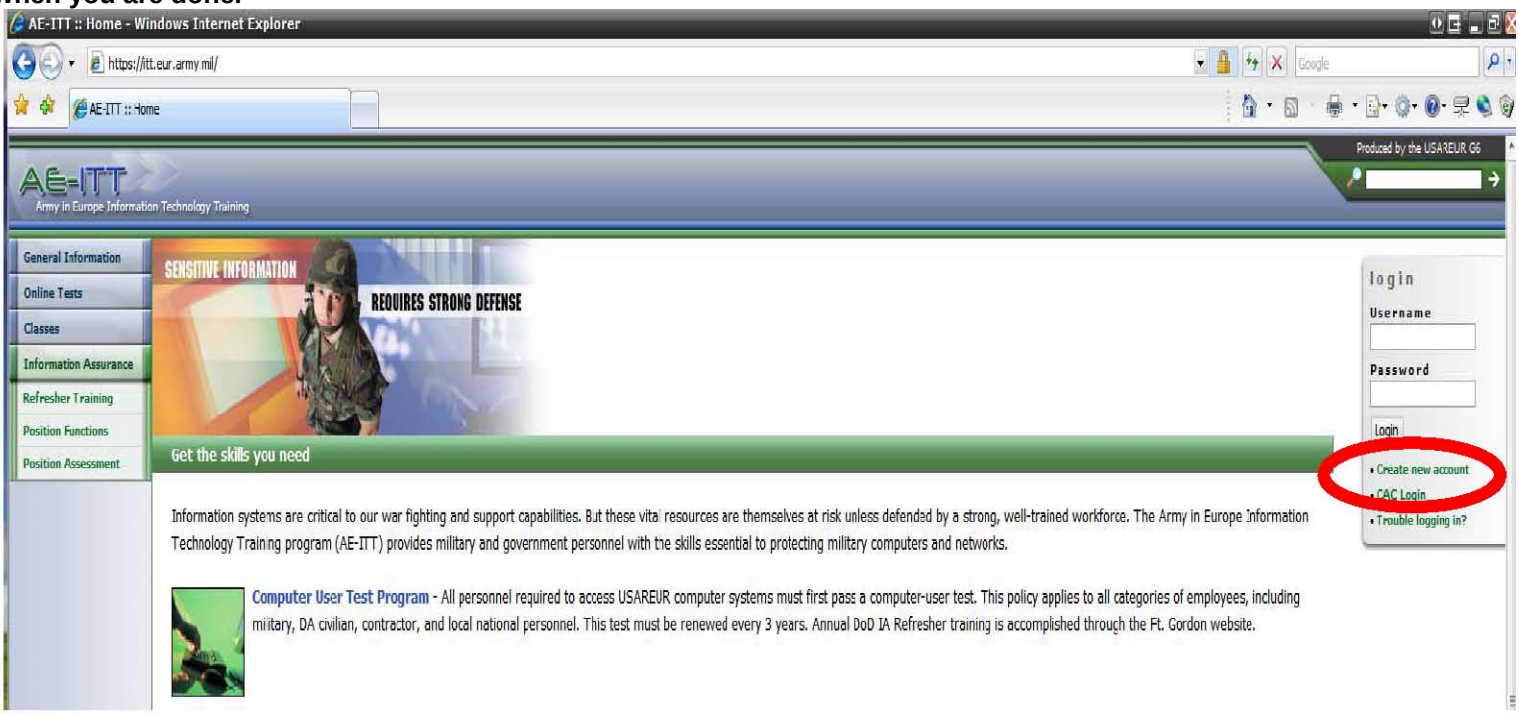
2 **AKO email address** – Go to https://www.us.army.mil to register if you do not have an AKO address.

3. Background Check – In accordance with AR 25-2 all users must have a favorable review. There is an ongoing initiative to standardize how USAREUR organizations document this part of the "create new account" process. Your sponsor will need to help you identify what form your organization requires. Many organizations have adopted the use of DD Form 2875 and instructions for that form follow.

Note: A CAC is required to access the AE-ITT website so you will need your sponsor to help you by connecting to the site for you. The sponsor should "cancel" the popup window asking for the CAC card credentials. This will allow the new user to select "Create New Account" (see screenshot, below).

3 **Computer User Test** – Go to https://itt.eur.army.mil and register for an account. This website requires CAC logon so you will have to have your sponsor logon to the UATP website. After registering, take the Online Computer User test.

4 **DoD Information Assurance Awareness Training Requirement** – **Go to https://ia.gordon.army.mil/DODIAA/DEFAULT.asp , or alternatively access the same link via the Refresher Training link at AE-ITT. Make sure you login to the site to take the training so that you can print a copy of your certificate when you are done.**



AE-ITT :: Home - Windows Internet Explorer

https://itt.eur.army.mil/

AE-ITT :: Home | Home - Wiesbaden ROC

Produced by the USAREUR G6

AE-ITT

Army in Europe Information Technology Training

General Information

Online Tests

Classes

Information Assurance

Refresher Training

Position Functions

Position Assessment

SENSITIVE INFORMATION

REQUIRES STRONG DEFENSE

Get the skills you need

Information systems are critical to our war fighting and support capabilities. But these vital resources are themselves at risk unless defended by a strong, well-trained workforce. The Army in Europe Information Technology Training program (AE-ITT) provides military and government personnel with the skills essential to protecting military computers and networks.

login

Username

Password

Login

- Create new account
- CAC Login
- Trouble logging in?

AE-ITT :: DOD Information Assurance Refresher Training - ALARACT 293/2007 - Windows Internet Explorer

https://itt.eur.army.mil/NewsStory.aspx?ID=61

Links | _Kia | _USAG-W | Active Directory | AE | Army | ASG | Buy Stuff | CAC | Digbend-Printers | DoD | DOIM | Federal | GPC | IA | JCE | JOBS | MCP | MP | MyStuff

AE-ITT :: DOD Information Assurance Refresher Train...

Page - Tools -

Produced by the USAREUR G6

AE-ITT

Army in Europe Information Technology Training

General Information

Online Tests

Classes

Information Assurance

Refresher Training

Position Functions

Position Assessment

DOD Information Assurance Refresher Training - ALARACT 293/2007

Posted: 28 Jan 2008

PLEASE NOTE: As of 25 January 2008, the Army in Europe Computer User Security Awareness (refresher) training and exam have been replaced with the DoD Information Assurance Awareness training and exam. All previous Computer User Security Awareness certificates will be valid until the expiration date (12 months after taking the exam). Once the Computer User Security Awareness certificate expires, you will need to take the DoD Information Assurance Awareness training and exam to update your certificate.

Army CIO/G6 IAD is working to provide the management and tracking capability through ALMS at Ft Gordon, until such time as this tool becomes operational IAMs will be required to track their respective commands for this annual AR 25 2 requirement.

Go to **https://ia.gordon.army.mil/DODIAA/DEFAULT.asp** to complete the annual Information Assurance Awareness Training

Related Downloads

- **ALARACT 293 2007** ALARACT 293 2007
- **Signed Memo DoD IA Awareness Tng Req** Signed Memo DoD IA Awareness Training Requirement

LastUpdated: 2/20/2008 10:29:30 AM

Usage Policy - Privacy & Security - Accessibility - Powered by ActiveForce v2.0 - Copyright © 2000 Moestkin Systems LLC

login

Username

Password

Login

- Create new account
- CAC Login
- Trouble logging in?

Trusted sites

100%

Information Assurance Training Center - Windows Internet Explorer

https://ia.gordon.army.mil/DODIAA/DEFAULT.asp

Information Assurance Training Center

Information Assurance Training Center

School of Information Technology, Fort Gordon, Georgia

IA Home | Login | Courses | Workshops | Resources | U.S. Army | AKO

DoD Information Assurance Awareness Training

Objectives: The objectives of this training are listed as follows.

- Affect physical security of computer hardware and software.
- Limit access to computer equipment to authorized users only.
- Prevent computer fraud, waste and abuse.
- Implement effective contingency planning.
- Report security problems to the chain of command.
- Protect computer files from infection by malicious logic.

Additional Information: To successfully pass this training, students must receive 70% or greater on the exam. Once the exam is passed, students will have a certificate of completion (see Login Page for information on printing certificates). Certificates for the DoD Information Assurance Awareness training are valid for **12 months**.

To complete the annual Information Assurance Awareness Training, you must perform each of the following steps:

1. Click the *Launch DoD Information Assurance Awareness* link below to begin your training session. The training session will open in a new browser window. Once you complete the training, print the DoD IA Awareness annual certificate (**PLEASE NOTE:** If you do not print the DoD certificate, OR if you lose the DoD certificate, we will not be able to send you a copy. We only track your exam scores and can only provide you a certificate if you have successfully completed an exam, which is done in Step 3 below). **For Army requirements**, close the training session window and move on to Step 2.
2. Once you complete the training module, read the Army Addendum (**there will be questions on the exam related to the Army Addendum**).
3. After you have read the Army Addendum, take the DoD Information Assurance Awareness Exam.
   PLEASE NOTE: The exam must be taken with a passing score of 70% to meet Army IA annual training requirements. If you do not take and pass the DoD Information Assurance Awareness exam, your annual IA awareness training will not be recorded and will not be considered complete. You must take and pass the exam to receive the approved certificate from Fort Gordon.

The contents below are derived from the DoD Information Assurance Support Environment (DISA sponsored) web site.

If you are having trouble viewing the training module, Click Here

DoD Information Assurance Awareness

Launch Guided Tour

Launch DoD Information Assurance Awareness

Continue Current DoD Information Assurance Awareness

This site was created by the Information Assurance Division of Fort Gordon, Georgia. Copyright 2007 All Rights Reserved

This site can be best viewed with a screen resolution of 1024 x 768 or higher, using the most current versions of Internet Explorer, Netscape, Mozilla Firefox and Opera

Privacy and Security Notice | Disclaimer | Contact Webmaster

DD Form 2875 – There is a blank form at the end of this document or you can go to http://www.dlis.dla.mil/PDFs/DD2875.pdf for an electronic version of the form.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

(See page 6 for Instructions)

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. None. Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request. AUTHORITY: PRINCIPAL PURPOSE: ROUTINE USES: DISCLOSURE:

TYPE OF REQUEST INITIAL MODIFICATION DEACTIVATE USER ID	DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications)	LOCATION (Physical Location of System)

PART I (To be completed by Requestor)

1. NAME (Last, First, Middle Initial)		2. SOCIAL SECURITY NUMBER
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. PHONE (DSN or Commercial)
6. OFFICIAL E-MAIL ADDRESS	7. JOB TITLE AND GRADE/RANK	
8. OFFICIAL MAILING ADDRESS	9. CITIZENSHIP US FN OTHER	10. DESIGNATION OF PERSON MILITARY CIVILIAN CONTRACTOR

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required. **USER AGREEMENT**

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) I have completed Annual Information Awareness Training. DATE (YYYYMMDD) ☐

11. USER SIGNATURE	12. DATE (YYYYMMDD)

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.) 14. TYPE OF ACCESS REQUIRED: AUTHORIZED PRIVILEGED 13. JUSTIFICATION FOR ACCESS ☐☐

15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED (Specify category) OTHER ☐☐☐

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)

26a. NAME (Last, First, Middle Initial)	26b. SOCIAL SECURITY NUMBER

27. OPTIONAL INFORMATION (Additional information)

PART III SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION LEVEL ☐ Level I ☐ Level II ☐ Level III	
29. VERIFIED BY (Print name)	30.Security Manager Phone Number	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Social Security Number. The social security number of user.

(3) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(4) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(5) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(6)Official E-mail Address. The user's official e-mail address.

(7) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(8) Official Mailing Address. The user's official mailing address.

(9) Citizenship (US, Foreign National, or Other).

(10) Designation of Person (Military, Civilian, Contractor).

IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.
(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

Computer-User Agreement

APPENDIX A COMPUTER-USER AGREEMENT This agreement is also available on the Army In Europe Information Training Program website at https://itt.eur.army.mil/. Your information management officer (IMO), system administrator (SA), or information assurance security officer (IASO) will ask you to sign a copy of this agreement before issuing you login credentials (user-ID and password). As a user of information systems in the Army in Europe, I will adhere to the security requirements outlined in DOD, Army, and Army in Europe policy, in particular the information assurance (IA) policy described in AE Pamphlet 25-25, with special attention directed to the following:

1 I will use Army information systems (computers, systems, and networks), operating systems, and programs only when authorized and only for authorized purposes.
2 I understand that my use of Government communications systems and networks serves as consent to authorized auditing and monitoring.
3 I will not install software or install or move hardware on any Government computer (GC) or network without the written approval from my IMO, SA, IASO, or (in the case of major changes) my designated approving authority.
4 I understand that the use of employee-owned information systems or devices on an Army in Europe network is prohibited, as is the processing, storage, or transmission of sensitive official information on such systems.
5 I know I will be issued a user-ID and password to authenticate my computer account. After receiving them—

a. I am responsible for all activity that occurs on my individual account. If I am a member of an authorized group account, I am responsible for all activity when I am logged onto a system with that account.
b. I will not allow anyone else to have or use my password. If I suspect that my password iscompromised, I will report this immediately to my SA.
c. I will not forward chain e-mail (example: rewards from various companies by simply forwarding an e-mail message). I will report chain e-mail, or virus warnings to my IAO and delete the message.
d. I will ensure my password meets length and complexity requirements by comprising a total of at least 10 characters, with at least 2 lowercased letters, 2 uppercased letters, 2 numbers, and 2 special characters.
e. I will ensure that my NIPRNET and (if applicable) SIPRNET passwords are changed at least once every 90 days and changed immediately if compromised.
f. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it accordingly.

1 I will ensure that the antivirus software on my GC is updated at least weekly, and I will scan all e-mail attachments, other media, and other devices for malicious code before opening attachments or using the devices on a GC or on an Army in Europe network.
2 I will not use Internet “chat” services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If a chat service is required, I will use my AKO account.
3 I know that if connected to the SIPRNET, my system operates in the U.S. or NATO (as applicable) Secret “system-high” mode.

a. I will not enter information into a system if the information has a higher classification than that for which the system and network are accredited. If the information is proprietary or requires other special protection, I will seek guidance from my IASO.
b. I will protect all data and output at the system-high level unless or until the information is downgraded or declassified by authorized personnel using appropriate procedures. I understand that U.S. classified information must be marked and protected according to AR 380-5, and that NATO material must be marked and protected according to AR 380-15.
c. Classified magnetic disks, compact disks, and other media will not be removed from the work area without the approval of the local commander or head of the organization.
d. If working in a classified area, I will ensure that only U.S. personnel with appropriate security clearances are allowed unescorted access to the systems.
e. If working in a classified area, I will ask my IASO about TEMPEST (Red/Black) separation requirements for system and network components, and I will ensure that those requirements are met.

f. I will use only approved methods to “air-gap” information to and from the SIPRNET.

1 I understand and will comply with the Public Key Infrastructure (PKI) requirements in AE Regulation 25-1-5 with regard to digitally signing and encrypting e-mail.
2 I will not attempt to defeat or bypass system or network security controls.
3 I know what constitutes a security incident or inadequate security and that I must immediately report such occurrences to my IASO.
4 I understand the information and requirements as presented in AE Pamphlet 25-25 and in this agreement, and will

execute my responsibilities to keep my system and the network secure. If I am a supervisor, IMO, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.

5 I know I am subject to disciplinary action if I violate DOD, Army, or Army in Europe computer security policy.

Computer-User Name			Security Officer Name
(Typed or Printed):		(Typed or Printed):	
Computer-User Signature:		Security Officer Signature:	
Date:		Date:	

ANHANG A

VEREINBARUNG ZUR COMPUTERNUTZUNG

Die hier abgedruckte Vereinbarung ist außerdem auf der Webseite des Army In Europe Information Training Program website at https://itt.eur.army.mil/ veröffentlicht.

Der für Sie zuständige Information Management Officer (IMO) (Beauftragter Informationsverarbeitung und -übermittlung), System Administrator (SA)

(Systemverwalter), oder Information Assurance Security Officer (IASO) (Beauftragter Informationssicherheit) wird Sie vor Ausstellung von Berechtigungsnachweisen zur Anmeldung im Computer bzw. Netzwerk (Benutzerkennung und Kennwort) bitten, eine Kopie dieser Vereinbarung zu unterzeichnen.

Als Benutzer eines von der US-Army in Europa eingerichteten Informationssystems verpflichte ich mich, die vom US-Verteidigungsministerium, der US-Army und der USArmy in Europa aufgestellten Sicherheitsvorgaben einzuhalten, insbesondere die in AE Pamphlet 25-25 enthaltenen Vorgaben zur Informationssicherheit. Besonders beachten werde ich dabei Folgendes:

1 Ich werde die Informationssysteme der US-Army (Computer, Systeme und Netzwerke), Betriebssysteme und Programme nur mit ausdrücklicher Genehmigung und nur für die genehmigten Zwecke benutzen.
2 Mir ist bekannt, dass ich mit meiner Benutzung der Kommunikationssysteme und Netzwerke der USRegierung meine Zustimmung zur genehmigten Nutzungsanalyse und Überwachung gebe.
3 Ich werde weder Software auf einem regierungseigenen Computer oder Netzwerk installieren ohne vorher die schriftliche Genehmigung des für mich zuständigen IMO, SA oder IASO bzw. (im Falle größerer Veränderungen) meiner Designated Approving Authority eingeholt zu haben, noch werde ich ohne deren Genehmigung Hardware installieren oder umstellen.
4 Mir ist bekannt, dass die Verwendung eigener Informationssysteme oder Mittel auf einem Netzwerk der US-Army in Europa untersagt ist, ebenso die Verarbeitung, Speicherung und Übermittlung sensitiver dienstlicher Informationen auf solchen Systemen.
5 Ich weiß, dass mir zur Authentisierung meines Benutzerkontos eine Benutzer-Identifikation und ein Kennwort ausgestellt werden. Nach Zuweisung meiner Benutzer-Identifikation und meines Kennworts werde ich

a. die Verantwortung für alle Vorgänge, die auf meinem Konto stattfinden, übernehmen. Sofern ich ein Benutzerkonto mit anderen Mitarbeitern teile, werde ich die Verantwortung für alle Vorgänge übernehmen, die auf diesem Konto stattfinden, während ich in dem System, auf dem sich das Benutzerkonto befindet, angemeldet bin;
b. mein Kennwort nicht an Dritte weitergeben oder Dritten erlauben, dieses zu benutzen. Habe ich den Verdacht, dass die Vertraulichkeit meines Kennwortes nicht mehr länger gewährleistet ist, werde ich umgehend den für mich zuständigen SA informieren;
c. sicherstellen, dass mein Kennwort den Vorgaben bzgl. Anzahl und Art von Zeichen entspricht, d.h. mindestens aus 10 Zeichen besteht und mindestens 2 Kleinbuchstaben, 2 Großbuchstaben, 2 Zahlen und 2 Sonderzeichen enthält;
d. dafür Sorge tragen, dass mein Kennwort fürs NIPRNET bzw. (gegebenenfalls fürs) SIPRNET mindestens alle 90 Tage geändert wird bzw. sobald seine Vertraulichkeit nicht länger gewährleistet ist;
e. mein Kennwort entsprechend schützen, falls sich mein Benutzerkonto auf einem klassifizierten Netzwerk befindet. Mir ist bekannt, dass die Einstufung meines Kennwortes der auf diesem Netzwerk gespeicherten Daten zu entsprechen hat.

1 Ich werde sicherstellen, dass die auf meinem Computer installierte Antivirensoftware mindestens

einmal pro Woche aktualisiert wird und ich werde alle E-Mail Anhänge, andere Datenträger und Mittel durch Scanning auf Malicious Codes hin überprüfen, bevor ich die Anhänge öffne oder die Mittel auf einem Computer oder Netzwerk der USArmy in Europa nutze.

2 Ich werde keinen Internet Chat-Dienst (wie z. B. America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) von dem mir bereitgestellten Computer aus nutzen. Bei Bedarf werde ich lediglich den auf meinem Army Knowledge Online (AKO) Benutzerkonto nutzen.

3 Mir ist bekannt, dass bei Anschluss ans SIPRNET mein System auf Geheimhaltungsstufe (US oder gegebenenfalls NATO), entsprechend der Einstufung des Systems arbeitet.

a. Ich werde keine Daten ins System eingeben, deren Einstufung höher ist als die, für die das System oder das Netzwerk zugelassen ist. Vor Eingabe von urheberrechtlich geschützten oder speziell zu schützender Daten werde ich meinen IASO um entsprechende Weisung bitten.

b. Ich werde Daten und Datenausgaben auf der höchsten Einstufung schützen, es sei denn bzw. bis die Daten durch dazu berechtigte Personen unter Anwendung der angemessenen Verfahren freigegeben oder herabgestuft sind. Mir ist bekannt, dass US klassifizierte Informationen und Daten gemäß AR 380-5 und NATO-Dokumente gemäß AR 380-15 zu kennzeichnen und zu schützen sind.

c. Klassifizierte magnetische Disketten, CDs und andere Datenträger sind ohne Genehmigung des örtlichen Kommandeurs bzw. Dienststellenleiters nicht vom Arbeitsbereich zu entfernen.

d. Arbeite ich in einer Classified Area, werde ich sicherstellen, dass nur USBedienstete mit entsprechender Ermächtigung zum Zugriff auf klassifizierten Daten bzw. zum Zugang zu Classified Areas ohne Begleitung Zugang zu den Systemen erhalten.

e. Arbeite ich in einer Classified Area, werde ich mich bei meinem IASO nach den einzuhaltenden Vorgaben bzgl. des TEMPEST-Standards (Red/Black) für Systeme und Netzwerk erkundigen und ich werde sicherstellen, dass diese Vorgaben eingehalten werden.

f. Ich werde nur zugelassene Verfahren verwenden, um Informationen mittels des Air-Gapping Verfahrens aufs und vom SIPRNET zu übertragen.

1 Mir sind die Public Key Infrastructure (PKI) Vorgaben in AE Regulation 25-1-5 bzgl. digitaler Signatur und Verschlüsselung von E-Mails bekannt und ich werde sie einhalten.

2 Ich werde nicht versuchen, für die Systeme bzw. Netzwerke eingerichtete Sicherheitskontrollen zu deaktivieren oder zu umgehen.

3 Ich weiß, welche Vorfälle eine Sicherheitsverletzung oder Sicherheitslücke darstellen, und dass ich diese umgehend dem für mich zuständigen IASO zu melden habe.

4 Ich habe die Informationen und Vorgaben in AE Pamphlet 25-25 und in dieser Vereinbarung zur Kenntnis genommen und verpflichte mich, zur Sicherheit meines Systems und des Netzwerks verantwortungsbewusst beizutragen. Sollte ich die Position eines Vorgesetzten, IMO, SA oder IASO bekleiden, verpflichte ich mich darüber hinaus sicherzustellen, dass alle Computerbenutzer in meinem Verantwortungsbereich diese Vereinbarung unterzeichnen.

5 Ich bin mir darüber im Klaren, dass ein Verstoß gegen die vom USVerteidigungsministerium, der US-Army und der US-Army in Europa aufgestellten Vorgaben zur Computersicherheit zu Disziplinarmaßnahmen führen kann.

Name des Computernutzers: Name des Sicherheitsbeauftragten:

(Maschinen- oder Blockschrift) _____ (Maschinen- oder Blockschrift) _____

Unterschrift des Unterschrift des

Computernutzers : _____ Sicherheitsbeauftragten : _____

Datum: _____ Datum: _____