

21 May 2004

Abt. Informationsverarbeitung und Informationsübermittlung

**Army in Europe Leitfadens über die Nutzung der Informationstechnologie**

---

\*Dieses Merkblatt ersetzt *AE Pamphlet 25-25-G* vom 18. September 2003.

---

For the CG, USAREUR/7A:

E. PEARSON  
Colonel, GS  
Deputy Chief of Staff

Official:



GARY C. MILLER  
Regional Chief Information  
Officer - Europe

---

**Zusammenfassung:** Dieses Merkblatt dient als Leitfadens für die Benutzung der von der US-Regierung am Arbeitsplatz bereitgestellten Informationstechnologie (IT) (siehe Glossar). Zur Gewährleistung des Schutzes und der Sicherheit von Informationen enthält das Merkblatt Vorgaben für die Benutzung regierungseigener Computer, die den Schutz vor Computerviren und Hackern sicherstellt.

**Zusammenfassung der Änderungen:** Dieses Merkblatt beinhaltet neue Vorgaben des US-Verteidigungsministeriums sowie der US-Landstreitkräfte zur Informationssicherung.

**Geltungsbereich:** Die Vorgaben dieses Merkblattes gelten für alle bei den US-Landstreitkräften in Europa Beschäftigten (Militär- und Zivilbedienstete), die an ihrem Arbeitsplatz von der US-Regierung bereitgestellte Computer benutzen.

**Formblätter:** *AE* Formblätter und Formblätter höherer Dienststellen sind über das *Army in Europe Publishing System (AEPUBS)* zu beziehen.

**Dokumentation:** Unterlagen, die aufgrund eines in dieser Dienstvorschrift vorgeschriebenen Verfahrens erstellt wurden, sind gemäß den Vorgaben in *AR 25-400-2* zu kennzeichnen, aufzubewahren und zu vernichten. Aktenzeichen und die zur Titelaufnahme erfaßten Angaben können auf der Webseite des *Army Records Management Information System* unter <https://www.armis.army.mil> abgerufen werden.

**Verbesserungsvorschläge:** Die Verantwortung für dieses Merkblatt liegt bei *USAREUR G6 (AEAIM-IAPM, DSN 380-5220)*. Verbesserungsvorschläge sind auf Formblatt *DA Form 2028* an *USAREUR G6 (AEAIM-IAPM), Unit 29351, APO AE 09014-9351* zu richten.

**Verteiler:** A (*AEPUBS*).

## INHALTSVERZEICHNIS

1. Zweck
2. Ihr Computer als Zugang zu Informationen und zum Internet
3. Welcher Bedrohung sind Computer ausgesetzt?
4. Nutzung regierungseigener Computer
5. Meldung von Sicherheitsverletzungen
6. Der richtige Umgang mit Ihrem Computer
7. Test
8. Zusammenfassung

### Anhang

- A. Vereinbarung über die Computernutzung

### Glossar

---

## 1. ZWECK

a. Als Benutzer eines von der US-Regierung bereitgestellten Computers können Sie durch Ihre Handlungsweise die Sicherheit unserer Netzwerke sowohl positiv als auch negativ beeinflussen. Der Schutz von Informationen und Daten auf diesen Netzwerken wird als *Information Assurance* (dt. Informationssicherung) bezeichnet. Der vorliegende Leitfaden stellt Ihr Benutzerhandbuch für die Daten-Autobahn, die „Infobahn“, dar und zeigt auf, wie Sie Risiken, denen Sie bei der Benutzung dieser Infobahn ausgesetzt sind, erkennen und durch die richtige Handlungsweise vermeiden.

b. Vor Ausstellung einer Zugangsberechtigung zur Infobahn haben Sie den von den US-Landstreitkräften in Europa geforderten Test zur Computernutzung (Abs. 7) abzulegen und eine Vereinbarung zur Computernutzung (Anhang A) zu unterschreiben. Mit Ihrer Unterschrift unter diese Vereinbarung verpflichten Sie sich, das Netzwerk verantwortungsbewußt zu nutzen und die vom Kommando aufgestellten Richtlinien zur Computernutzung zu befolgen. Die zum erfolgreichen Ablegen des geforderten Tests notwendigen Informationen finden Sie in diesem Leitfaden.

## 2. IHR COMPUTER ALS ZUGANG ZU INFORMATIONEN UND ZUM INTERNET

a. Da fast alle bei den US-Landstreitkräften in Europa benutzten, nicht-eingestuften Computer über Netzwerke miteinander verbunden sind, haben Sie Zugriff zu fast jedem nicht-eingestuften Computer innerhalb des Verantwortungsbereichs des US-Verteidigungsministeriums. Im Gegenzug haben die Benutzer dieser Computer allerdings auch Zugriff zu Ihrem Computer. Da andere vom US-Verteidigungsministerium bereitgestellte Computer Ihrem Computer „vertrauen“, haben Sie Zugriff zu Informationen, die von diesem Ministerium veröffentlicht werden, der breiten Öffentlichkeit aber nicht zugänglich sind. Außerdem sind fast alle ans *LandWarNet (Unclass)* (nicht klassifiziertes Netzwerk) angeschlossenen Computer auch ans kommerzielle Internet angeschlossen. Das *LandWarNet (Class)* (klassifiziertes Netzwerk) ist zwar nicht ans kommerzielle Internet angeschlossen, dient aber der Verbindung aller innerhalb des Verantwortungsbereichs des US-Verteidigungsministeriums bereitgestellten Computer zum Austausch von Informationen. Ausgetauscht werden dabei alle möglichen Informationen bis hin zu als geheim eingestuften Informationen.

b. Durch diese Vernetzung von Computern haben Sie über Ihren Computer Zugriff zu einer Fülle von Informationen. Diese Vernetzung setzt Ihren Computer allerdings auch Risiken aus, die von allen Computern ausgehen können, die mit Ihrem vernetzt sind. Als Benutzer eines von der US-Regierung bereitgestellten Computers bei den US-Landstreitkräften in Europa kommt Ihnen deshalb eine Schlüsselrolle zu, was den Schutz unserer Daten betrifft.

## 3. WELCHER BEDROHUNG SIND COMPUTER AUSGESETZT?

Viren- und Wurmprogramme, Hacker, aber auch Militär- oder Zivilbedienstete der US-Streitkräfte oder der US-Regierung können eine Bedrohung für den von Ihnen am Arbeitsplatz genutzten Computer darstellen.

a. Viren- und Wurm-Programme sind Programme, die auf dem Computer gespeicherte Programme und Daten verfälschen und/oder schädigen. Ein Programm muß nicht unbedingt Schadensfunktionen durchführen, um ein Virus- bzw. ein Wurmprogramm zu sein. Es reicht, wenn die Viren-bzw. Wurm-Programme andere Programme infizieren oder ändern. Die meisten Viren-Programme enthalten allerdings Schadensfunktionen, die z. B. Daten von Ihrem Laufwerk löschen. Wurm-Programme können ein auf Ihrem Computer gespeichertes Programm in einer Weise ändern, die es Hackern erlaubt, uneingeschränkten Zugriff zu Ihrem Computer zu erhalten bzw. ihn als „Wirt“ zum Infizieren anderer Computer zu benutzen.

b. Das Öffnen einer aus unbekannter Quelle stammenden, infizierten E-Mail bzw. einer der E-Mail angehängten Datei ist gegenwärtig die gängigste Methode der Verbreitung von Viren. Sie sollten nie Ihren Computer so einrichten, daß E-Mail-Nachrichten automatisch in einer Vorschau angezeigt werden.

c. Falsche Warnungen vor Viren-Programmen, sog. Scherznachrichten oder Falschmeldungen (*Hoaxes*), werden allerdings häufiger verschickt als tatsächliche Viren-Programme. Viele Warnungen vor angeblichen Viren und andere Falschmeldungen bedienen sich Pseudofachausdrücken oder einer gefühlsbetonten Sprache. Sie bieten z. B. Tips an, wie man schnell zu Geld kommt, oder appellieren an Ihr Mitgefühl, heben beispielsweise die Dringlichkeit der Nachricht hervor und fordern Sie auf, die Warnung unbedingt sofort an alle möglichen Leute weiterzuleiten, damit diese sich vor einem verheerenden Virus schützen können.

d. Die vorsätzliche Installation eines Programms mit Schadensfunktion (so der Fachausdruck für Viren-Programme und andere Programme, die Daten und Programme schädigen und verfälschen) auf einem Informationssystem der US-Regierung stellt einen Verstoß gegen einen rechtmäßigen Befehl gemäß des *Uniform Code of Military Justice (UCMJ)* (US-Militärkodex), Artikel 92, dar. Bedienstete, die dem *UCMJ* nicht unterliegen, können sich nach dem *United States Code* (offizielle Sammlung von US-Bundesgesetzen), US-Rechtsverordnungen oder rechtlichen Bestimmungen des Aufnahmestaates strafbar machen. Hacker versuchen regelmäßig Sicherheits-Schwachstellen in der Betriebssoftware Ihres Computers zu finden, um ins System einzudringen. Oft geschieht dies mittels eines Viren- oder Wurmprogramms.

e. Am Besten ist es, erst gar nicht zuzulassen, daß sich Viren auf Ihrem Computer einnisten. Als Computerbenutzer der US-Landstreitkräfte in Europa können Sie durch folgende fünf Präventivmaßnahmen zum angemessenen Schutz ihrer Computer und der darauf gespeicherten Informationen beitragen:

- Stellen Sie sicher, dass die auf dem Ihnen von der US-Regierung bereitgestellten Computer installierte Antiviren-Software stets auf dem neuesten Stand ist. Gemäß Vorgaben der US-Landstreitkräfte in Europa ist die Antiviren-Software mindestens einmal pro Woche zu aktualisieren. Das gleiche gilt für die auf *Personal Digital Assistants (PDAs)* (Taschencomputer) und *Personal Electronic Devices (PEDs)* (Taschencomputer) (eigene und von der Regierung bereitgestellte) installierte Antiviren-Software.

**ANMERKUNG:** In den meisten Dienststellen der US-Landstreitkräfte in Europa wird die auf den regierungseigenen Computern installierte Antiviren-Software automatisch aktualisiert. Außerdem kann die vom US-Verteidigungsministerium erworbene Antiviren-Software von Militär- und Zivilbediensteten der US-Streitkräfte auf ihren Computern zu Hause installiert werden.

- Die *USAREUR Computer Security Baseline* muß von Ihrem *Information Management Officer (IMO)* (Sicherheitsbeauftragter, Informationsverarbeitung und –übermittlung) bzw. *Information Assurance Security Officer (IASO)* (Sicherheitsbeauftragter, Informationssicherung) installiert und aktualisiert werden.
- Achten Sie auf ungewöhnliche Betriebsweisen des Computers und melden diese (s. Abs. 5).
- Melden Sie sich am Ende des Arbeitstags aus dem System ab.
- Stellen Sie Ihren Computer so ein, dass beim Durchsuchen der Dateien nach Viren alle Dateien überprüft werden.

f. Selbst die besten Vorkehrungen können allerdings das Auftreten von Viren nicht verhindern. Viren sind auch nicht immer sofort zu erkennen. Folgendes könnte u. a. ein Hinweis darauf sein, daß ein Computer durch einen Virus infiziert ist:

- Ungewöhnliche Bildschirmanzeigen und –meldungen
- Eine langsamere Arbeitsweise des Computers
- Ungewöhnliche Aktivitäten, Fehlermeldungen, Änderungen in der Dateigröße, Verlust von Programmen bzw. Daten

#### **4. NUTZUNG REGIERUNGSEIGENER COMPUTER**

##### **a. Schutz und Sicherung regierungseigener Computer**

(1) Die Ihnen zur Benutzung am Arbeitsplatz bereitgestellten Computer sind Eigentum der US-Regierung und sind in erster Linie für dienstliche Zwecke zu nutzen. Darüberhinaus können die Computer in dem genehmigten Umfang für private Zwecke sowie in begrenztem Umfang im Rahmen der Betreuungsprogramme zum Zweck der Kommunikation zwischen verlegten Soldaten/innen und ihren Familienangehörigen benutzt werden. Alle Computerbenutzer haben

- sämtliche Informationssysteme und die darauf gespeicherten Informationen gegen Sabotage, Manipulation, Lahmlegung (*Denial-of-Service*) und Spionage zu schützen und dürfen sie unter keinen Umständen Personen, die keine Berechtigung zur Nutzung dieser Computer bzw. Informationen haben, überlassen bzw. zugänglich machen;

- Hardware, Software und Dokumente unter Verschuß zu halten. Die Einstufung der Hardware, Software und Dokumente hat dabei der höchsten Stufe der darauf gespeicherten Daten zu entsprechen;
- Sicherheitsverletzungen, Schwachstellen und Virenattacken dem für sie zuständigen *System Administrator* (SA) (Systemverwalter) oder *IASO* zu melden;
- alle magnetischen Datenträger (z. B. Disketten, Kompaktdisketten (CDs), Bänder, *USB<sup>1</sup> Memory Sticks* (USB-Speichermodule)) vor deren Nutzung auf einem regierungseigenen Computer, einem Informationstechnologie- (IT) System oder einem Computernetzwerk der US-Landstreitkräfte in Europa auf Software mit Schadensfunktion (z. B. auf Viren- und Wurmprogramme) hin zu überprüfen.
- mit dem für Sie zuständigen *IASO* Verbindung aufzunehmen, um sicherzustellen, daß ihr System den neuesten Informationen bezüglich des *Information-Assurance-Vulnerability-Alert (IAVA)* (Programm zur Überwachung und Behebung von Sicherheitslücken) entspricht, wenn der ihnen von der US-Regierung bereitgestellte Computer vom Netzwerk getrennt war (z. B. wenn sie ihr Laptop zum Arbeiten über das Wochenende mit nach Hause genommen haben oder von einer Dienstreise zurückkehren).

(2) Soldaten, die gegen diese Vorgaben verstoßen, haben gemäß § 92 des *Uniform Code of Military Justice (UCMJ)* (US-Militärkodex) mit Verwaltungs- und Disziplinarmaßnahmen zu rechnen. Personen, auf die der *UCMJ* keine Anwendung findet, können sich nach dem *United States Code*, US-Rechtsverordnungen oder rechtlichen Bestimmungen des Aufnahmestaates strafbar machen.

**ANMERKUNG:** Ortsansässige Arbeitnehmer unterliegen nicht dem *United States Code* bzw. US-Rechtsverordnungen. Auf sie finden rechtliche Bestimmungen des Aufnahmestaates Anwendung.

**b. Genehmigte private Nutzung:** In welchem Umfang die von der US-Regierung bereitgestellten Computer für private Zwecke genutzt werden können, ist in der *Joint Ethics Regulation (JER) (DOD Reg 5500.7)*, Paragraph 2-301, sowie in *AR 25-1* festgelegt. Danach darf ein Arbeitnehmer den ihm von der US-Regierung bereitgestellten Computer unter anderem dazu benutzen, um für kurze Zeit ins Internet zu gehen und Informationen im Internet zu suchen, sowie um kurze Nachrichten über E-Mail zu verschicken. Gemäß *JER* sind Kommandeure und Vorgesetzte verpflichtet sicherzustellen, daß die Benutzung der regierungseigenen Computer für private Zwecke der Ausführung der dienstlichen Aufgaben nicht abträglich ist. Regierungseigene Computer können für private Zwecke benutzt werden, wenn die Nutzung

- gemäß den Vorgaben des US-Verteidigungsministeriums und denen der US-Landstreitkräfte in Europa erfolgt;
- auf eine angemessene Dauer und Häufigkeit begrenzt ist und, wenn möglich, vor oder nach der regulären Arbeitszeit erfolgt;
- nicht zu beträchtlichen Zusatzkosten für das US-Verteidigungsministerium bzw. die US-Landstreitkräfte führt und diese nicht in ein negatives Bild rückt;
- einem legitimen öffentlichen Interesse dient, z. B. zur Ausbildung und Weiterbildung der Beschäftigten beiträgt oder die Moral und das Wohlergehen der Beschäftigten hebt bzw. fördert. Arbeitnehmern kann es auch gestattet werden, die bereitgestellten Computer bei Personalabbau zur Arbeitssuche zu nutzen. Die Nutzung regierungseigener Computer zum Versenden von Nachrichten zwischen verlegten Soldaten/innen und ihren direkten Angehörigen per E-Mail ist zulässig und wird von den US-Landstreitkräften in Europa in großem Maße gefördert;
- zu keiner Überlastung des Kommunikationssystems führt. Denken Sie stets daran: Das militärische Kommunikationssystem (innerhalb dessen das *LandWarNet (Unclas)* eine wichtige Rolle spielt) wurde in erster Linie zur Unterstützung der Soldaten/innen eingerichtet.

### c. Kennwörter

(1) Ihr Kennwort ist Ihr „Schlüssel“ zur Daten-Autobahn. Er eröffnet allerdings nicht nur Ihnen den Zugang zur riesigen Welt verschiedenener militärischer Netzwerke und der des Internet. Dieser Schlüssel gewährt gleichzeitig auch anderen Zugriff zu denselben Informationen. Als Benutzer eines von der US-Regierung bereitgestellten Computers wird Ihnen für jedes Benutzerkonto, das Ihnen ausgestellt wird, eine nur von Ihnen zu verwendende und einmalig ausgestellte Benutzererkennung sowie ein solches Kennwort zugewiesen. Der Schutz Ihres Kennwortes zählt deshalb zu den wichtigsten Sicherheitsvorkehrungen, die Sie als Computerbenutzer treffen müssen. Sie allein tragen die Verantwortung für den Schutz Ihres Kennwortes und jeder E-Mail-Nachricht, die von Ihrem Benutzerkonto verschickt wird. Erhält jemand Kenntnis Ihres Kennwortes, könnte er es benutzen und in der virtuellen Welt unter Ihrem Namen auftreten. Sie tragen die Verantwortung für alles, was unter der Benutzererkennung und dem Kennwort, unter dem Sie sich auf einem regierungseigenen Computer im Datennetz anmelden, geschieht. Geben Sie deshalb Ihr Kennwort nie an Dritte weiter. Die Befolgung folgender Richtlinien trägt zum Schutz Ihres Kennwortes bei:

<sup>1</sup> Datenleitung zum Anschluß peripherer Geräte

- Halten Sie Ihr Kennwort nicht schriftlich fest oder lassen gar einen Zettel mit Ihrem Kennwort an Ihrem Arbeitsplatz offen herumliegen bzw. hängen diesen auf;
- Speichern Sie Ihr Kennwort nicht online oder auf einem *PDA* bzw. *PED*. Geben Sie Ihr Kennwort auch unter keinen Umständen in einer E-Mail-Nachricht an;
- Stellen Sie sicher, daß Ihr Kennwort nicht auf dem Bildschirm erscheint, wenn Sie sich in Ihrem Computer anmelden;
- Stellen Sie sicher, daß Ihr Kennwort bei Nutzung des *LandWarNet (Unclass)* alle 150 Tage bzw. bei Nutzung des *LandWarNet (Class)* alle 90 Tage geändert wird. Ist die Vertraulichkeit Ihres Kennwortes nicht länger gewährleistet, melden Sie dies umgehend dem für Sie zuständigen SA und lassen sich ein neues ausstellen.
- Befindet sich Ihr Benutzerkonto auf einem klassifizierten Netzwerk, ist Ihr Kennwort entsprechend der höchsten Einstufung der auf diesem Netzwerk gespeicherten Daten eingestuft und auf dieselbe Weise zu schützen wie klassifizierte Daten.

(2) Bei den US-Landstreitkräften in Europa können Kennwörter entweder vom Benutzer selbst erstellt werden oder werden vom zuständigen *IMO* ausgestellt. Folgende Vorgaben gelten dabei für Kennwörter:

- **Vom Benutzer erstellte Kennwörter** haben aus mindestens 10 Zeichen zu bestehen, wobei mindestens je zwei Großbuchstaben, zwei Kleinbuchstaben, zwei Zahlen und zwei Sonderzeichen sein müssen. Kennwörter dürfen keine Wörter bilden und dürfen mit den 10 zuletzt benutzten Kennwörtern nicht identisch sein. Entspricht Ihr Kennwort nicht den gültigen Vorgaben US-Landstreitkräfte in Europa, sollten Sie umgehend Ihrem SA Meldung machen.
- **Vom *IMO* ausgestellte Kennwörter** sind nach dem Zufallsprinzip zu erstellen und haben ebenfalls 10-stellig zu sein. Die Kennwörter haben einen alphanumerischen Code zu bilden und aus mindestens zwei Großbuchstaben, zwei Kleinbuchstaben, zwei Zahlen und zwei Sonderzeichen zu bestehen.

(3) Lassen Sie Ihren Computer nie unbeaufsichtigt, während Sie unter Ihrem Benutzernamen angemeldet sind, es sei denn, Ihr Computer ist mittels eines Bildschirmschoners mit zugewiesenem Kennwort geschützt.

#### **d. Nutzung des *LandWarNet (Class)***

(1) Jeder an das *LandWarNet (Class)* (klassifiziertes Netzwerk, s. Abs. 2a) angeschlossene Computer arbeitet zumindest auf Geheimhaltungsstufe (US), entsprechend der Einstufung des Systems. Alle auf diesem System benutzten magnetischen Datenträger sowie alle Ausdrücke sind umgehend gemäß *AR 380-5* zu kennzeichnen und zu überwachen bzw. zu schützen, und zwar bis zur Freigabe oder Herabstufung der Daten mittels eines zugelassenen Verfahrens. Das bedeutet, jede Diskette, die in ein als „Geheim“ eingestuftes System eingelegt wird, ist als „Geheim“ einzustufen und entsprechend zu handhaben. Schreibgeschützte Datenträger sind als „Geheim“ zu kennzeichnen und mit dem entsprechenden Etikett zu versehen. Klassifiziertes NATO-Material ist ebenfalls gemäß *AR 380-5* zu kennzeichnen und zu überwachen bzw. zu schützen.

(2) Nicht in ein System einzugeben sind Daten, die

(a) höher eingestuft sind als das System oder

(b) den US-Landstreitkräften eigen, von Mitarbeitern verpflichteter Privatfirmen nicht zu nutzen oder anderweitig speziell zu schützen oder zu handhaben sind.

(3) Nur US-Bediensteten, die als „Geheimnisträger“ Zugriff zu Verschlusssachen haben, ist zu Systemen, die an das *LandWarNet (Class)* angeschlossen sind, ohne Begleitung Zugang zu gewähren. Magnetdisketten bzw. Disketten sind von solchen Systemen ohne ausdrückliche Genehmigung des zuständigen Kommandeurs oder Dienststellenleiters nicht zu entfernen. Der für Sie zuständige *IASO* sollte Sie über die nach *TEMPEST* zu treffenden Vorkehrungen informieren. Nach *TEMPEST (Red/Black)* sind Systemkomponenten (eingestufte und nicht-eingestufte) voneinander zu trennen, um eine unzulässige Überwachung zu vermeiden. Hardware und andere IT-Geräte dürfen deshalb nur mit Genehmigung des zuständigen *IASO* umgestellt werden.

(4) Nicht-amerikanischen Staatsbürgern ist kein Zugang zu Bereichen mit *LandWarNet (Class)*-Ausstattung zu gewähren. Nicht-amerikanische Staatsbürger, denen Zugang zu US-kontrollierten Bereichen gewährt wurde, sind anzumelden und ständig zu begleiten; Bildschirme sind zu verdecken. Ist nicht-amerikanischen Staatsbürgern Einblick auf Bildschirme gestattet, haben die US-Bediensteten sicherzustellen, daß die einzusehenden Daten auch an diese Personen weitergegeben werden können. Einem nicht-amerikanischen Staatsbürger ist zu keiner Zeit Kontrolle über ein *LandWarNet (Class)*-Terminal zu gewähren.

(5) Nicht-klassifizierte Daten können vom *LandWarNet (Unclas)* oder *LandWarNet (Class)* unter Nutzung des sogenannten „Air-gapping“<sup>2</sup>-Verfahrens übertragen werden. Informationen zu genehmigten Verfahren erteilt Ihr *IASO*.

**e. Nutzung der *Public Key Infrastructure* Zertifikate:** Wurde auf Ihrem Computer ein *Public Key Infrastructure (PKI)* Zertifikat installiert (z. B. Software Token), haben Sie sicherzustellen, dass dieses entfernt wird, wenn dafür kein Bedarf mehr besteht. Besteht für das Zertifikat kein Bedarf mehr, sollten Sie umgehend Ihren *SA* sowie den zur Ausstellung berechtigten Vertreter der örtlichen Registrierungsstelle informieren.

**f. Zugelassene Software und Hardware:** Die auf regierungseigenen Computern installierte Software und Hardware muß zugelassen und ihre Installation vom jeweiligen Kommandeur, *IASO* und *IMO* genehmigt sein. Die Original-Software ist an einem sicheren Ort aufzubewahren, z. B. in einem abgeschlossenen Schrank oder in einer abgeschlossenen Schublade. Ohne vorherige schriftliche Genehmigung des zuständigen Kommandeurs, *IASO*, *SA* und *IMO* darf keine Software auf regierungseigenen Computern installiert werden. Das Gleiche gilt für den Anschluß jeglicher Art von Hardware an ein Netzwerk der US-Landstreitkräfte in Europa (einschl. *PDA*s und *PED*s, wie z. B. *Palm Pilots*). Ist die Installation einer Software auf einem regierungseigenen Computer erforderlich, so sind vor der Installation der zuständige *IASO* und *SA* entsprechend zu informieren und deren Genehmigung einzuholen. Eigene IT-Mittel (Hardware und Software) können für dienstbezogene Arbeiten am Arbeitsplatz verwendet werden, vorausgesetzt der zuständige Kommandeur und die *Designated Approving Authority (DAA)* (genehmigende Instanz) genehmigen diese Verwendung. Auf allen *PDA*s und *PED*s (eigene und von der US-Regierung bereitgestellte) ist die vom US-Verteidigungsministerium zugelassene Antiviren-Software zu installieren.

**g. Benutzung der *Army Knowledge Online (AKO)*:** Militärangehörige, Zivilbedienstete und Mitarbeiter verpflichteter Privatfirmen, denen ein E-Mail-Benutzerkonto der US-Landstreitkräfte in Europa ausgestellt werden kann, haben sich außerdem ein Webmail-Benutzerkonto des Online-Dienstes der US-Army, *AKO*, ausstellen zu lassen. Alle anderen Webmail-Dienste sind für dienstliche Kommunikationszwecke bei den US-Landstreitkräften in Europa nicht zu nutzen. *AKO* bietet darüberhinaus einen Internet Chat-Dienst an, der auf dem *LandWarNet (Unclas)* als einziger genutzt werden kann. Jegliche Nutzung anderer kommerzieller Chat-Dienste ist untersagt. Die Dienststellenleitung hat für ortsansässige Arbeitnehmer als „Sponsor“ für die *AKO*-Benutzerkonten zu fungieren.

**h. Gesperrte Webseiten:** Die US-Landstreitkräfte in Europa haben das sog. *WebSense*-Programm eingeführt, das einen Zugriff zu gesperrten Webseiten (z. B. zu solchen mit pornographischem und hetzerischem Inhalt) nicht erlaubt und außerdem den Zugang zum Internet für private Zwecke einschränkt. In Ausnahmefällen kann Zugang zu diesen Webseiten genehmigt werden. Arbeitnehmer, die Zugang wünschen, haben sich mit dem für sie zuständigen *IASO* in Verbindung zu setzen.

**i. Untersagte Aktivitäten:** Als Computerbenutzer sind Sie am besten in der Lage, jede unzulässige Computernutzung zu unterbinden. In der *JER* und in einschlägigen Vorgaben der US-Landstreitkräfte in Europa ist genauestens festgelegt, welche Computer-Software nicht zu verwenden ist und welche Nutzung der Computer-Netzwerke einen Mißbrauch darstellt. Im Folgenden sind die wichtigsten Vorgaben hierzu (ohne prioritäre Zuordnung) aufgeführt sowie Aktivitäten, die auf den Netzwerken der US-Landstreitkräfte in Europa untersagt sind. Untersagt ist bzw. sind

- Vorhandensein und/oder Besitz und die Installation verbotener Software auf regierungseigenen Computern. Nicht verwendet werden dürfen *Peer-to-Peer File-Sharing Software*, wie z. B. MP3 Musik und Video-Software; das sog. *Streaming*, wodurch Audio- und Video-Dateien bereits während der Übertragung, also in Echtzeit, angehört bzw. angeschaut werden können; Dateien der *Moving Picture Experts Group (MPEG)*; Hacker-Programme und Hilfssoftware; Software zur Entwicklung von Schadenslogik und Wurmprogrammen, ausführbare Programme (d.h. mit „.exe“ gekennzeichnete Dateien) sowie Makros; Programme zur Überwachung des Umgangs der Nutzer mit dem Netzwerk und ihrer Tastatureingaben; nicht-zugelassene Software (Raubkopien); Software zum Ändern von Webseiten; Spiele (einschl. *America's Army*); eigene *Firewalls* (einschl. vom US-Verteidigungsministerium zugelassener und Windows XP *Internet Connection Firewalls*) sowie jede andere vom Kommandeur der Einheit und dem zuständigen *IMO* nicht zugelassene Software;
- die Nutzung kommerzieller Internet Chat-Dienste wie *America Online (AOL)* *Instant Messenger* zum Austausch von Kurznachrichten in Echtzeit, *Yahoo Chat* sowie Webseiten, die Chat-Dienste anbieten. Einziger zugelassener Chat-Dienst auf dem *LandWarNet (Unclas)* ist der von *AKO*;
- die Nutzung vernetzter IT-Mittel bzw. regierungseigener Computer zur persönlichen Bereicherung oder für illegale Handlungen;
- Versuche, Computernetzwerke oder Sicherheitskontrollen auszureizen, zu testen oder zu umgehen;
- Versuche, ohne entsprechende ausdrückliche Genehmigung Zugriff zu Daten zu erhalten oder Betriebssysteme bzw. Programme zu verwenden;

---

<sup>2</sup> Anschlußmäßige Trennung von ans Internet und ans interne Netzwerk angeschlossenen Computern

- die Überwachung des Umgangs der Nutzer mit dem Netzwerk und ihrer Tastatureingaben ohne offizielle Genehmigung;
- die Änderung bzw. Manipulation der auf regierungseigenen Computern installierten Software und Hardware ohne Genehmigung des zuständigen SA, IASO oder IMO;
- ein Umstellen regierungseigener Computer ohne Genehmigung des SA, IASO oder IMO, zumal die meisten Schäden an Computern durch bzw. beim Umstellen entstehen;
- die Installation von Computer-Viren und –Würmern, Schadenscodes in IT-Mittel oder Netzwerke;
- die Weitergabe von Benutzerkennungen oder Kennwörtern;
- das Speichern, Bearbeiten, Aufrufen, Versenden oder anderweitiges Übermitteln von Material mit anstößigem bzw. obszönem Inhalt, wie z. B. von Literatur mit rassistischem, sexuell explizitem, beleidigendem oder hetzerischem Inhalt;
- das Speichern oder Bearbeiten eingestufte Information auf einem System (einschl. PEDs und PDAs), das für die Bearbeitung von Verschlusssachen nicht zugelassen ist;
- das Speichern und Bearbeiten von urhebergeschütztem Material (einschl. Cartoons), es sei denn es liegt dafür die Genehmigung des Autors oder Verlags vor;
- die unberechtigte Einsichtnahme, Änderung, Beschädigung oder das unerlaubte Löschen von Dateien anderer Computerbenutzer sowie das Blockieren des Zugangs dieser Computerbenutzer zu ihren Dateien oder anderen Verbindungen;
- der Erwerb, die Installation, das Kopieren, Speichern oder Nutzen von Software unter Verletzung des Lizenzvertrages des jeweiligen Vertreibers;
- das Überlassen eines von der US-Regierung bereitgestellten Computers oder eines von ihr betriebenen Netzwerks einer zur Nutzung nicht berechtigten Person;
- Versuche, illegal in das Netzwerk von USAREUR einzudringen bzw. von diesem illegal in andere Netzwerke einzudringen (hacken);
- das Verschicken oder Weiterleiten offizieller E-Mail-Nachrichten von einem an das LandWarNet (Unclas) angeschlossenen Computer an ein durch einen kommerziellen Internet-Anbieter (wie z. B. AOL, Compuserve, Hotmail, Yahoo) bereitgestelltes E-Mail-Konto;
- die Verwendung der Benutzerkennung und des Kennwortes eines Dritten sowie Verschleierung der eigenen Identität;
- die Installation und Verwendung eines Modem ohne Genehmigung des zuständigen DAA;
- das Verfassen und Weiterleiten von Kettenbriefen und Falschmeldungen;
- die Veröffentlichung privater Homepages;
- die Nutzung eines regierungseigenen Computers zur persönlichen Bereicherung;
- das Herunterladen bzw. Laden lizenzfreier Software;
- der gleichzeitige Anschluß eines regierungseigenen Computers an ein von der US-Regierung betriebenes Netzwerk und einen kommerziellen Internet-Anbieter;
- der gleichzeitige Anschluß eines regierungseigenen Computers an das LandWarNet (Unclas) und einen kommerziellen Internet-Anbieter mittels eines PED- oder PDA-Modems.

#### **j. Zustimmung zur Nutzungsanalyse und Überwachung**

(1) Unter engl. „Auditing“ (dt.: Revision oder Nutzungsanalyse) versteht man die unabhängige Überprüfung und Untersuchung von Unterlagen und Aktivitäten. Eine Nutzungsanalyse wird durchgeführt, um die Funktion von Systemen und der zu ihrer Kontrolle entwickelten Verfahren zu überprüfen, die Einhaltung der vorgegebenen Bestimmungen und Betriebsverfahren sicherzustellen und Empfehlungen hinsichtlich notwendiger Änderungen dieser Kontrollverfahren, Bestimmungen und Betriebsverfahren zu geben. Alle Handlungen und Aktivitäten von Personen, die Zugriff aufs LandWarNet (Unclas) oder LandWarNet (Class) haben, unterliegen einer solchen Überwachung.

(2) In der Regel sind sich alle Angehörigen und Beschäftigten der US-Landstreitkräfte, die von der US-Regierung bereitgestellte Kommunikationssysteme benutzen, darüber im Klaren, daß mit jedweder Nutzung der Systeme, ob genehmigt oder nicht, zufällig oder privat, gleichzeitig eine Zustimmung zur Überwachung gegeben wird. Wenn Sie auf dem Warnhinweis, der beim Start Ihres Computers auf dem Bildschirm erscheint, auf OK klicken, geben Sie damit Ihre Zustimmung zur Überwachung Ihres Computers am Arbeitsplatz. Mit der Überwachung regierungseigener Computer soll sichergestellt werden, daß jegliche Nutzung genehmigt ist und alle Computerbenutzer die vorgegebenen Sicherheitsbestimmungen beachten. Unter anderem dient die Überwachung zur Kontrolle, zur Rekonstruktion von Aktivitäten auf dem Benutzerkonto sowie zur Erfassung aller Versuche, Sicherheitsmechanismen zu umgehen.

**k. Eingeschränkte Nutzung:** Während Zeiten erhöhter Netzwerkaktivität können die US-Landstreitkräfte in Europa gezwungen sein, Aktivitäten, die zur Erfüllung des Auftrags der US-Landstreitkräfte nicht wesentlich sind, auf den Netzwerken einzuschränken. Wird eine eingeschränkte Nutzung (MINIMIZE) der Computernetzwerke angeordnet, dürfen die von der US-Regierung bereitgestellten Computer für die Dauer der Anordnung nicht für private Zwecke genutzt werden. Ausgenommen ist eine Nutzung regierungseigener Computer

- zum Austausch von E-Mail-Nachrichten zwischen verlegten Soldaten/innen und ihren Familienangehörigen. Die Einheiten sind angehalten, den Familienunterstützungsgruppen die Computer in den Büros zugänglich zu machen, damit diese, unter Aufsicht, die von der US-Regierung eingerichteten Netzwerke zum Austausch von E-Mail-Nachrichten mit Soldaten, die zur Unterstützung von Operationen der Vereinten Nationen, NATO und des US-Kommandos Europa (*USEUCOM*) verlegt wurden, benutzen können;
- im Rahmen von Ausbildungs- bzw. Schulungsmaßnahmen und –programmen der US-Landstreitkräfte bzw. anderer zugelassener Bildungs-/Ausbildungszentren sowie im Rahmen von Programmen, die zu einem Hochschulabschluß führen;
- im Rahmen der Betreuungsprogramme;
- für Aktivitäten der dem US-Verteidigungsministerium unterstellten Schulen, vorausgesetzt, die Schüler werden von einem Erwachsenen beaufsichtigt.

## 5. MELDUNG VON SICHERHEITSVERLETZUNGEN

a. Vorfälle, die Ihrer Meinung nach eine Sicherheitsverletzung darstellen könnten, sind dem für Sie zuständigen SA oder IASO unverzüglich zu melden. Verletzt wird die Sicherheit von Computern und Computersystemen durch Verstöße gegen ausdrückliche oder implizite Sicherheitsbestimmungen. Im Folgenden sind einige Beispiele für solche Sicherheitsverletzungen aufgeführt:

- Versuche (erfolgreiche oder fehlgeschlagene), unberechtigten Zugriff zu einem System bzw. der auf ihm gespeicherten Daten zu erhalten (d. h. zu hacken);
- Versuche (erfolgreiche oder fehlgeschlagene), Systeme zur Kontrolle von Computernetzwerken oder Sicherheitskontrollen zu deaktivieren oder zu umgehen (Bsp.: Deaktivierung oder Umgehung des WebSense-Programms oder von Kennwörtern etc.);
- Herunterladen von MP3 Dateien oder einer anderen nicht zugelassenen Software;
- Verfassen oder bewußtes Übertragen eines Computer-Virus oder –Wurms oder einer anderen Logik mit Schadensfunktion;
- Weiterleiten von Kettenbriefen per E-Mail.

b. Außerdem haben Sie unverzüglich Meldung zu machen, wenn Sie den Eindruck haben,

- ein Virus hätte sich auf Ihrem Computer eingenistet;
- Hacker hätten versucht bzw. versuchen, sich Zugriff zu Ihrem Computer zu verschaffen;
- eine genehmigte bzw. erforderliche Aktivität auf dem Netzwerk funktioniere nicht richtig.

c. Haben Sie den Verdacht, Ihr Computer sei durch einen Virus oder Wurm infiziert oder weise eine eigenartige Betriebsweise auf, dann

- schalten Sie Ihren Computer auf keinen Fall aus,
- ziehen Sie das Netzkabel aus dem Computer (Das Kabel sieht aus wie ein Telefonkabel) und
- rufen den für Sie zuständigen SA bzw. IASO an. Sind diese nicht erreichbar, rufen Sie die Hotline des *Regional Emergency Response Team, Europe* (Computer-Notfall-Team in Europa) an, Tel.: 380-5232.

## 6. DER RICHTIGE UMGANG MIT IHREM COMPUTER

Um eine einwandfreie Betriebsweise zu gewährleisten, haben Sie mit Ihrem Computer sorgsam umzugehen.

- Essen und trinken Sie nicht in unmittelbarer Umgebung Ihres Computers. Limonade, Kaffee und andere Flüssigkeiten, die auf dem Computer verschüttet werden, können zu Schäden an Computer und Dateien führen.
- Halten Sie Ihr System sauber und staubfrei.
- Trennen Sie Ihren Computer nie vom Netz (es sei denn, sie haben Grund zur Annahme, daß er durch einen Virus infiziert ist). Die kleinen Anschlußstecker sind nicht allzu stabil und sehr teuer.
- Stellen Sie Ihren Computer nur im Beisein des für Sie zuständigen SA oder IASO um.
- Schalten Sie Ihren Computer am Ende Ihres Arbeitstages ab, es sei denn Sie haben ihn aufgrund entsprechender Anweisungen des für Sie zuständigen SA oder IMO zur IAVA-Aktualisierung angeschaltet zu lassen. Zu abgeschalteten Geräten können Hacker keinen Zugriff erhalten. Ein Abschalten mindert auch das Risiko eines Feuersausbruchs.
- Setzen Sie Ihren Computer keiner extremen Hitze, Kälte oder Luftfeuchtigkeit aus.

## 7. TEST

a. Nun, da Sie diesen Leitfaden gelesen haben, verfügen Sie über alle Informationen, die Sie zur Beantwortung der im Rahmen des Tests zur Computernutzung gestellten Fragen benötigen. Um den Test abzulegen, rufen Sie ihn bitte auf der *Information Assurance Computer-User Test* Webseite unter <https://www.uatp.hqusaeur.army.mil> auf und melden sich für den Test an.

b. Nach erfolgreichem Ablegen des Tests wird Ihnen umgehend eine „Zulassung“ ausgestellt (*Information Assurance Computer-User License*), die Sie berechtigt, die Infobahn der US-Landstreitkräfte in Europa zu benutzen. Die Zulassung ist 3 Jahre gültig. Sollten Sie nach Ablauf dieser 3 Jahre weiterhin die Infobahn der US-Landstreitkräfte in Europa benutzen, haben Sie den Test erneut abzulegen, bevor Ihnen eine neue Zulassung ausgestellt werden kann.

c. Vor Ausstellung eines Benutzerkontos und eines Kennwortes für den Ihnen bereitgestellten Computer wird der für Sie zuständige *IMO* oder *IASO* Sie bitten, die *Computer User Agreement* (Vereinbarung über die Computernutzung) (Anhang A) zu lesen und zu unterschreiben. Mit Ihrer Unterschrift bestätigen Sie, die von der US-Army und den US-Landstreitkräften in Europa zur Benutzung regierungseigener Computer getroffenen Regelungen zur Kenntnis genommen zu haben, und verpflichten sich, diese einzuhalten. Mit Ihrer Unterschrift übernehmen Sie gleichzeitig die Verantwortung und Nachweispflicht für alle Vorgänge, die auf Ihrem Benutzerkonto stattfinden. Bei Verweigerung Ihrer Unterschrift unter diese Vereinbarung wird Ihnen kein Benutzerkonto für eines der Computernetzwerke der US-Landstreitkräfte in Europa ausgestellt.

d. Von dem Moment an, da Sie sich im System anmelden, können Sie die Vorteile der Infobahn genießen, tragen aber gleichzeitig auch die Verantwortung, die mit der Benutzung der Infobahn verbunden ist. Die Benutzung der Infobahn ist mit Risiken verbunden und Sie sind verpflichtet, den von Ihnen benutzten Computer und das Netzwerk vor diesen Risiken durch eine angemessene Vorgehensweise zu schützen. Denken Sie stets daran: Der vorliegende Leitfaden ist Ihr Benutzerhandbuch für die Infobahn. Bewahren Sie deshalb eine Kopie des Leitfadens bei Ihrem Computer oder in einer Ihrer Ablagen im Büro auf.

## 8. ZUSAMMENFASSUNG

Als Benutzer eines regierungseigenen Computers kommt Ihnen, was die Sicherheit, Erhaltung, Verfügbarkeit und Vertraulichkeit von Daten der US-Landstreitkräfte in Europa betrifft, eine Schlüsselrolle zu. Mit der Befolgung der im Vorangegangenen erläuterten Maßnahmen stellen Sie die Sicherheit Ihres regierungseigenen Computer und aller Netzwerke, an die Ihr Computer angeschlossen ist, sicher. Damit schützen Sie nicht nur sich selbst, sondern das gesamte Kommando. Zur Erinnerung seien die wichtigsten zu beachtenden Punkte nochmals wiederholt:

- Halten Sie Ihr Kennwort unter Verschuß!
- Stellen Sie sicher, daß Ihre Antiviren-Software stets auf dem neuesten Stand ist!
- Befolgen Sie die bzgl. der Computernutzung für private Zwecke getroffenen Regelungen!
- Melden Sie dem für Sie zuständigen SA bzw. IASO Viren sowie alle Vorfälle, die die Netzwerksicherheit beeinträchtigen könnten!

## ANHANG A VEREINBARUNG ÜBER DIE COMPUTERNUTZUNG

Die in dieser Anlage abgedruckte Vereinbarung ist eine Kopie der auf der Webseite des *USAREUR Automation Training Program* (<https://www.uatp.hqusareur.army.mil>) veröffentlichten Vereinbarung über die Computernutzung. Der für Sie zuständige *System Administrator (SA)* (Systemverwalter) bzw. *Information Assurance Security Officer (IASO)* (Sicherheitsbeauftragter, Informationssicherung) wird Sie vor Ausstellung eines Kennwortes bitten, diese Vereinbarung zu unterzeichnen.

---

Als Benutzer eines von den US-Landstreitkräften in Europa eingerichteten Informationssystems verpflichte ich mich, die folgenden Sicherheitsvorschriften zu beachten:

1. Ich werde die Informationssysteme der US-Landstreitkräfte (Computer, Systeme und Netzwerke) nur für die genehmigten Zwecke benutzen.
2. Ich werde keine regierungseigene Software oder Hardware auf einem Computer (Arbeitsplatz- oder Zentralrechner) installieren, ohne vorher die schriftliche Genehmigung meines Kommandeurs, des für mich zuständigen SA oder IASO eingeholt zu haben.
3. Ich werde ohne ausdrückliche Genehmigung meines Kommandeurs, des für mich zuständigen SA oder IASO keine Software auf von der US-Regierung bereitgestellte Computer, Informationstechnologie (IT)-Systeme oder Netzwerke installieren.
4. Ich werde nie versuchen, zu Informationen Zugriff zu erhalten oder Betriebssysteme und Programme zu benutzen, wenn ich dazu nicht die ausdrückliche Genehmigung bzw. Berechtigung habe.
5. Mir ist bekannt, dass mir zur Authentisierung meines Kontos eine Benutzer-Identifikation zugewiesen und ein Kennwort ausgestellt wird. Nach Zuweisung meiner Benutzer-Identifikation und meines Kennwortes werde ich Folgendes beachten:
  - a. Ich werde mein Kennwort nicht an Dritte weitergeben oder Dritten erlauben, dieses zu benutzen. Ist die Vertraulichkeit meines Kennwortes nicht mehr länger gewährleistet, werde ich umgehend den für mich zuständigen SA informieren und mir ein neues ausstellen lassen.
  - b. Befindet sich mein Benutzerkonto auf einem klassifizierten System, werde ich dafür Sorge tragen, dass mein Kennwort mindestens alle 90 Tage geändert wird, bzw. sobald die Vertraulichkeit meines Kennwortes nicht länger gewahrt ist. Maßgeblich ist der zuerst eintretende Fall.
  - c. Befindet sich mein Benutzerkonto auf einem nicht-klassifizierten System, werde ich dafür Sorge tragen, dass mein Kennwort mindestens alle 150 Tage geändert wird, bzw. sobald die Vertraulichkeit meines Kennwortes nicht länger gewahrt ist. Maßgeblich ist der zuerst eintretende Fall.
  - d. Befindet sich mein Benutzerkonto auf einem klassifizierten Netzwerk, so ist mir bekannt, dass die Einstufung meines Kennwortes der auf diesem Netzwerk gespeicherten Daten entspricht und ich mein Kennwort entsprechend zu schützen habe.
  - e. Ich übernehme die Verantwortung für alle Vorgänge, die auf meinem Konto nach Anmeldung unter meinem Kennwort stattfinden, sofern ich der einzige Benutzer dieses Kontos bin. Teile ich ein Benutzerkonto mit anderen Mitarbeitern, trage ich die Verantwortung für alle Vorgänge, die auf diesem Konto stattfinden, während ich im System angemeldet bin.
  - f. Mir ist bekannt, dass ich den für mich zuständigen SA zu informieren habe, wenn mein Kennwort nicht den von den US-Landstreitkräften vorgegebenen Bestimmungen entspricht.
  - g. Ich werde mein Kennwort auf keinem Prozessor, Mikrocomputer, Taschencomputer (*Personal Digital Assistant (PDA)* oder *Personal Electronic Device (PED)*) oder irgendeinem magnetischen oder elektronischen Datenträger speichern.
  - h. Ich werde meinen Computer nicht manipulieren, um die Einhaltung der von den US-Landstreitkräften in Europa aufgestellten Bestimmungen über die Benutzung und den Umgang mit Kennwörtern zu umgehen.
  - i. Handelt es sich bei meinem Computer um ein klassifiziertes System, werde ich ihn nie unbeaufsichtigt lassen, während ich im System angemeldet bin, es sei denn, er ist mittels eines Bildschirmschoners mit zugewiesenem Kennwort geschützt.
6. Mir ist bekannt, dass Versuche, die eigene Identität zu verschleiern oder zu verbergen, oder die Identität eines anderen anzunehmen, einen Verstoß gegen die Bestimmungen zur Computernutzung darstellt.

7. Ich werde alle magnetischen Datenträger (Disketten, CDs, Bänder, USB *Memory Sticks* (Speichermodule) etc.) durch Scanning auf Software mit Schadensfunktionen (z. B. Viren- und Wurmprogramme) hin überprüfen, bevor ich diese auf einem Computer, IT-System oder Netzwerk der US-Landstreitkräfte in Europa installiere bzw. nutze.
8. Ich verpflichte mich, Kettenbriefe und falsche Warnhinweise auf Viren nicht weiterzuleiten. Außerdem verpflichte ich mich, dem für mich zuständigen *IASO* umgehend Meldung zu machen, sollte ich per E-Mail Kettenbriefe oder Warnhinweise auf Viren erhalten, und diese Nachrichten anschließend zu löschen.
9. Versuche, *Sniffer* oder andere von Hackern benutzte Software auf einem Computer, IT-System und Netzwerk der US-Regierung zu verwenden, werde ich unterlassen.
10. Ich werde keine *File-Sharing* Software (einschl. MP3 Audio- und Video-Dateien) oder Spiele auf von der US-Regierung bereitgestellte Computer, IT-Systeme oder Netzwerke laden.
11. Ich werde ohne die ausdrückliche schriftliche Genehmigung meines Kommandeurs, des für mich zuständigen *SA*, *IASO* oder *IMO* keine eigenen IT-Mittel (*PEDs* und *PDA*s (wie z. B. *Palm Pilots*), eigene Computer, *Digitally Enabled Devices*) an den mir von der US-Regierung bereitgestellten Computer oder an eines von ihr eingerichteten Netzwerk anschließen.
12. Ich werde sicherstellen, dass die auf meinem Computer installierte Antiviren-Software mindestens einmal pro Woche aktualisiert wird.
13. Ich werde keinen Internet Chat-Dienst (wie z. B. *America Online (AOL)*, *Microsoft Network (MSN)* *Instant Messenger*, *Yahoo*) am Arbeitsplatz nutzen. Bei Bedarf werde ich lediglich den von *Army Knowledge Online (AOK)* nutzen.
14. Vorfälle, die auf eine Sicherheitsverletzung und eine Sicherheitslücke im System schließen lassen, werde ich umgehend dem für mich zuständigen *IASO* melden. Mir ist bekannt, welche Vorfälle Sicherheitsverletzungen darstellen können und dass ich diese umgehend dem zuständigen *IASO* zu melden habe.
15. Ich verpflichte mich, die von dem für mich zuständigen *SA* bzw. *IASO* ausgegebenen Sicherheitsweisungen zu befolgen.
16. Wurde ein *Public Key Infrastructure (PKI)* Zertifikat auf meinem Computer installiert (z. B. ein Software-Token), habe ich dafür zu sorgen, dass dieses entfernt wird, sobald dafür kein Bedarf mehr besteht. Besteht für das Zertifikat kein Bedarf mehr, habe ich dies dem für mich zuständigen *SA* sowie dem zur Ausstellung berechtigten Vertreter der örtlichen Registrierungsstelle zu melden.
17. Ich habe die vorstehende Vereinbarung zur Kenntnis genommen und verpflichte mich, zur Sicherheit des Systems beizutragen. Sollte ich die Position eines Vorgesetzten, Gruppenleiters, *SA* oder *IASO* begleiten, verpflichte ich mich darüberhinaus sicherzustellen, dass alle Computerbenutzer in meinem Verantwortungsbereich diese Vereinbarung unterzeichnen.
18. Ich bin mir darüber im Klaren, dass ein Verstoß gegen die von den US-Landstreitkräften in Europa aufgestellten Vorgaben zur Computernutzung zu Disziplinarmaßnahmen führen kann. US-Bedienstete, die gegen die Vorgaben verstoßen, können nach Artikel 92 des *Uniform Code of Military Justice (UCMJ)* (US-Militärkodex) zur Verantwortung gezogen werden und haben mit Verwaltungs- und Disziplinarmaßnahmen zu rechnen. Bedienstete, die dem *UCMJ* nicht unterliegen, können sich nach dem *United States Code* (offizielle Sammlung von US-Bundesgesetzen), US-Rechtsverordnungen oder rechtlichen Bestimmungen des Aufnahmestaates strafbar machen.

Name des Computernutzers (Maschinen- oder Blockschrift): _____	Name des Sicherheitsbeauftragten (Maschinen- oder Blockschrift) _____
Unterschrift: _____	Unterschrift: _____
Datum: _____	Datum: _____

## GLOSSAR

### ABSCHNITT I ERKLÄRUNG DER ABKÜRZUNGEN

<i>AKO</i>	<i>Army Knowledge Online</i>
<i>AOL</i>	<i>America Online</i>
<i>CD</i>	<i>Compact Disk</i>
<i>DAA</i>	<i>Designated Approving Authority</i>
<i>DOD</i>	<i>Department of Defense</i>
<i>IASO</i>	<i>Information Assurance Security Officer</i>
<i>IAVA</i>	<i>Information Assurance Vulnerability Alert</i>
<i>IMO</i>	<i>Information Management Officer</i>
<i>IT</i>	<i>Informationstechnologie</i>
<i>JER</i>	<i>Joint Ethics Regulation</i>
<i>MPEG</i>	<i>Moving Picture Experts Group</i>
<i>NATO</i>	<i>North Atlantic Treaty Organization</i>
<i>PDA</i>	<i>Personal Digital Assistant</i>
<i>PED</i>	<i>Personal Electronic Device</i>
<i>PKI</i>	<i>Public Key Infrastructure</i>
<i>SA</i>	<i>System Administrator</i>
<i>UCMJ</i>	<i>Uniform Code of Military Justice</i>
<i>US</i>	<i>United States</i>
<i>USB</i>	<i>Universal Serial Bus</i>
<i>USAREUR</i>	<i>United States Army, Europe</i>
<i>USEUCOM</i>	<i>United States European Command</i>

### ABSCHNITT II BEGRIFFE

#### **Informationstechnologie (IT)**

Die Hardware, Firmware und Software, die als Teil eines Informationssystems zur Unterstützung der Informationsaufgaben des US-Verteidigungsministeriums genutzt wird. Dazu gehören Rechner, Telekommunikation, automatisierte Informationssysteme und automatisierte Datenverarbeitungssysteme. Unter IT versteht man jede Art von Hardware, Software und Firmware, die dazu dient, Daten oder Informationen zu sammeln, zu erstellen, weiterzugeben, zu berechnen, zu verbreiten, zu speichern und zu überwachen.

#### ***LandWarNet (Class)***

Klassifiziertes Netzwerk der US-Landstreitkräfte (früher als *SIPRNET* bezeichnet)

#### ***LandWarNet (Unclas)***

Nicht-klassifiziertes Netzwerk der US-Landstreitkräfte (früher als *NIPRNET* bezeichnet)