



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON WIESBADEN
UNIT 29623
APO AE 09096-0050

IMEU-WSB-ZA

16 JUN 09

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: US Army Garrison Wiesbaden Command Policy Letter 10, Information Assurance

1. References:

- a. AR 25-2, Information Assurance, 24 October 2007.
- b. AE Pamphlet 25-25, Information Technology Users Guide, 2 June 2006.
- c. AE Pamphlet 25-25-G, Leitfaden für die Nutzung der Informationstechnologie, 2 June 2006.
- d. AE Supplement 1 to AR 25-1, Army Knowledge Management and Information Technology, 28 April 2006.

2. Purpose: To establish the US Army Garrison Wiesbaden Commander's Information Assurance (IA) Policy.

3. Applicability: This policy applies to all military and civilian employees within the USAG Wiesbaden Area of Responsibility (AOR).

4. Cyber war is a war about "knowledge"; specifically, who knows what, when, where, and why? Our information systems are under attack every day. To defend our "knowledge" and the information systems we use everyday to support the warfighter, are to enforce IA standards and ensure that only trained personnel uses these networks and they remain vigilant. The following policy will help reduce the risks and improve the security of our information and information systems:

5. Responsibilities:

a. Commanders and directors will take actions to reduce risks to information and information systems under their control by enforcing IA policy, promptly resolving IA incidents, and maintaining accountability for IA implementation.

b. Garrison computer users will:

(1) Before being issued a computer-user account:

(a) Have a fully functioning common access card (CAC).

(b) Have an AKO email address.

(c) Have a completed background check with favorable review.

IMEU-WSB-ZA

SUBJECT: US Army Garrison Wiesbaden Command Policy Letter 10, Information Assurance

(d) Take and pass the USAREUR Computer User Test <https://www.itt.eur.army.mil> and DoD Information Assurance Awareness Training <https://ia.gordon.army.mil/dodiaa/default.asp>.

(e) Fill out a DD Form 2875 <http://www.dlis.dla.mil/PDFs/DD2875.pdf>, and sign a Computer-User Agreement.

(2) Comply with IA guidelines and report any suspicious computer activity to their Information Assurance Network Officer (IANO), Information Manager Officer (IMO), or IT Tier II Technician (ITT2T).

(3) Not tamper with or try to circumvent the system's security, and will not install software without their IANO's approval and IMO or ITT2T assistance.

(4) Turn off government computers (GC) at the end of the duty day with the following exceptions:

(a) Users will ensure IT systems (servers, desktops, and notebooks) are connected to the network and remained turned on every Wednesday of the week for scanning and maintenance purposes. Users will log off instead of turning off computers at the end of the day.

(b) Key staff personnel who require remote access to their systems via VPN for mission support have authorization to leave their systems on as needed.

(5) Bring any information system not connected to the network in over 21 days to the IMO or ITT2T for software patching and inspection before brought online.

(6) Bring all mobile devices (laptops, thumb drives, PDAs) to the IMO or ITT2T to have data-at-rest (DAR) applied and will complete the Army G3 Thumb Drive Awareness and Computer Security Training modules at the Army's virtual IA training center <https://iatraining.us.army.mil>.

c. Installation Campus Area Network (ICAN) Access.

(1) Only accredited government owned systems are allowed connection the garrison's ICAN. Accredited contractor-owned systems can connect if the contract requires the contractor to provide the system.

(2) Under no circumstances are non-accredited government, contractor owned systems and employee-owned devices (including, but not limited to personal computers, personal digital assistants, and personal thumb drives) allowed connection to the ICAN.

d. Information Assurance Vulnerability Management.

(1) Before connecting any computer system to an Army in Europe network, IMO's or ITT2T's will apply the appropriate computer-security baseline and any necessary software patches.

IMEU-WSB-ZA

SUBJECT: US Army Garrison Wiesbaden Command Policy Letter 10, Information Assurance

(2) The supporting Directorate of Information Management (DOIM) Operation Center has the authority to disconnect any garrison information system from the network found to be non-compliant with an IAVM or other vulnerability that poses a threat to the network. This system will remain offline until it brought into validated compliance.

e. Public Key Infrastructure (PKI). Organizations will protect sensitive official information using PKI. PKI enables:

(1) Users to protect information transmitted by e-mail.

(2) Users to transmit legally enforceable, tamperproof policy and requirements by e-mail.

(3) Users to verify the identity of the sender.

6. An information security risk accepted by one person is a risk imposed on all of us. I therefore expect everyone to be trained and remain vigilant to ensure our information and information systems are secured. Keep up your guard by using the USAREUR Information Assurance and Security (iAssure) website at <https://iassure.usareur.army.mil> to find current information and guidance about IA.

7. This policy memorandum supersedes all previous USAG Wiesbaden IA policy memorandums.

8. The point of contact for this memorandum is the Directorate of Information Management Information Assurance Manager, DSN: 314-337-7303.



JEFFREY W. DILL
COL, IN
Commanding

DISTRIBUTION:

A