



DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON ANSBACH
UNIT 28614
APO AE 09177

AMIM-ANG-ZA

21 June 2024

MEMORANDUM FOR All Military Personnel, Civilian Personnel, Family Members and Local Nationals Assigned and Attached to United States Army Garrison (USAG) Ansbach

SUBJECT: Command Policy Letter #14 - Information Security (INFOSEC)

1. References:

- a. AR 380-5 (Army Information Security Program), Revised 25 March 2022
- b. AR 25-1 (Army Information Technology), Revised 15 July 2019
- c. AR 25-2 (Army Cybersecurity), Revised 30 May 2019

2. Cyberspace is a warfighting domain. Commanders, directors, and other civilian and military leaders must secure and defend our network while enforcing accountability and ensuring readiness. To ensure USAG Ansbach networks are resilient and resistant to cyber threats, all users must embrace a culture of proactive cybersecurity, which must be driven by command emphasis.

3. Although technical capabilities play a crucial role in our defenses, most cyber-attacks that become incidents result from human error. To ensure the security of our information and properly defend against cyber threats, leaders must:

a. Integrate cybersecurity into all mission and training objectives, particularly for our expeditionary Forces to ensure we are ready to fight and maintain interoperability with our Allies and partners.

b. Execute cybersecurity awareness, discipline, and individual accountability through leader engagement and oversight and report all incidents or violations through unit information-systems-security managers (ISSM).

c. Protect Army information from compromise and exploitation. We must train our personnel to be aware of, avoid, and report cybersecurity and information threats.

d. Reinforce traits and attributes of a proactive cybersecurity philosophy. Proactive actions, such as ensuring individual training is current, directly support a ready and resilient cybersecurity culture.

e. Ensure all information system users register in the Army Training and Certification Tracking System (ATCTS). Every user is required to pass the annual Cybersecurity training and sign the Information Technology (IT) user agreement and both cannot be older than one year.

AMIM-ANG-ZA

SUBJECT: Command Policy Letter #14 - Information Security (INFOSEC)

f. Conduct new employee Network Acceptable Use briefings to familiarize new employees with the incident handling and reporting procedures in the USAREUR Area of Responsibility (AOR).

4. No personally owned, or government issued computer devices or portable electronic devices (PEDs) are allowed on the government owned network regardless of situation. PEDs include cell phones, smart phones, iPhones, tablets, and mp3 players.

5. Reporting is required in both technical and command channels. Cybersecurity incidents will be reported to the USAG Ansbach ISSM in accordance with USAREUR-AF Commander's Critical Information Requirements. As assistance, users are regularly emailed the USAG Ansbach's Cybersecurity Trifold that provides email and telephone numbers on how to respond to various incidents.

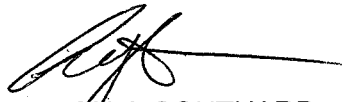
6. Failure to follow any of the above procedures, proper security and regulations will result in immediate suspension of network access and privileges.

7. Incident cleanup costs are considerable and often involve the sanitization or destruction of hard drives, computers, servers, other network components, and related labor costs. The costs increase rapidly as classified information is passed through the network if unauthorized disclosure of classified information (UDCI) are not immediately reported and contained. To offset the damage and cleanup costs associated with UDCIs, the unit/organization that originated the incident will pay the associated costs. Typical costs for units that originate a UDCI is at least \$5,000 per incident that does not require server cleanup, and at least \$10,000 per incident that requires server cleanup. UDCIs that require the impacted equipment be destroyed may cost significantly more.

8. The failure of any one unit, leader, or individual to secure our network, an information system, or hardware could compromise the USAG Ansbach mission. We must remain vigilant to prevent, detect, and report unauthorized activity. Cybersecurity ensures mission readiness and is everyone's responsibility. Please refer to the enclosure for "Information Security Definitions".

9. The POC is Ms. Diana Hanna, Information Management Officer at DSN 314-587-1540, commercial phone number 0611-143-587-1540 or email diana.m.hanna.ln@army.mil.

Encl


AARON J. SOUTHARD
COL, PO
Commanding

Enclosure: Information Security Definitions:

a. A cybersecurity incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information that system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b. Examples of cybersecurity incidents include, but are not limited to:

(1) Unauthorized disclosure of classified information (UDCI) or the synonymous common term "negligent discharge of classified information" (NDCI). UDCIs include, but are not limited to:

(2) Spillages: The introduction of classified information on a lower classified information system or a system with incompatible releasability restrictions. Spillages must be contained and sanitized from every component of the Department of Defense (DoD) enterprise that may be infected.

(3) Loss of any information system equipment or media containing sensitive or classified information.

(4) Cross Domain Violations (CDVs): The connection of a device and transfer of information on an information system that differs from its approved classification. CDVs typically occur when discipline is not properly enforced while moving a device connected to a DoD information system.

(5) Attempts to use or attach equipment and removable media (e.g., thumb drives, discs, etc.) not authorized for connection to DoD information systems. Such violations potentially introduce malware on a system.

(6) Attempts to access or collect data for which an individual has not been cleared.

(7) Attempts to circumvent information system access controls designed to protect sensitive or classified information.