DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON BAVARIA
UNIT 28130
APO AE 09114

AMIM-BAG-IM (1oo)

MEMORANDUM FOR All USAG Bavaria Military and Civilian Personnel

SUBJECT: USAG Bavaria Policy Memorandum #32, Cyber Policy Violations (CPV)

1. References:

a. DA PAM 25-2-17 (Incident Reporting).

b. AE Reg 25-2 (Army in Europe Information Assurance)

c. AE PAM 25-25 (Army in Europe Information Technology Users Guide)

d. USAREUR-AF (Incident Response Plan)

e. USAREUR-AF (Network Policy Violation [NPV] SOP)

2. All Garrison Professionals are responsible as the Army's first line of defense in evading and deterring undue cybersecurity risk across Army Europe networks and information systems. Steps to deterring this risk in USAG Bavaria are outlined in the Enclosure to this Memorandum.

3. POC for this policy is the USAG Bavaria DIT Cybersecurity Information Systems Security Manager (ISSM) at 526-6002 or usarmy.bavaria.id-europe.mesg.dit-cybersecurity@army.mil.

Encl

STEPHEN C. FLANAGAN
COL, SF
Commanding

d. If the offender is a Garrison employee and the incident is attributed to negligence or error, retraining must be completed before network access is reinstated.

(1) The supervisor conducts counseling and documents the event using DA Form 4856. Offenders are prohibited from using "DoD Visitor" access on Army IS until retraining is completed, and the incident is fully adjudicated.

(2) Supervisors will facilitate "proxy login" using a secondary, Garrison-issued CAC reader or CAC reader-equipped keyboard. The supervisor or a delegated employee will sign into the computer with their account and the offender will insert their CAC to the secondary reader. The offender selects their certificate(s) when prompted to apply digital signatures or authenticate to DoD websites.

(3) The offender will complete the Cyber Awareness Challenge at https://cs.signal.army.mil. Training conducted from any other source will not be accepted. The offender must save a copy of the completion certificate as a PDF.

(4) The offender will thoroughly review and sign the Army IT User Agreement at https://cs.signal.army.mil. Scroll to the bottom of the User Agreement webpage, digitally complete the form on the site. **Garrison personnel will select AMC as their Major Command (MACOM).** The offender must save a copy of the digitally signed agreement a as PDF.

(5) Offender will complete Using Mobile Devices in a DoD Environment Training at https://cyber.mil/training/dod-mobile-devices/#Information. The offender must save a copy of the completion certificate as a PDF.

e. The supervisor will submit DA Form 4856 (or Narrative Statement), Cyber Awareness Challenge certificate, Army IT User Agreement, and Mobile Devices in DoD Environment certificate to the USAG Bavaria DIT Cybersecurity Office.

f. The USAG Bavaria DIT Cybersecurity Office will complete the AE Form 25-2B Cyber Policy Violation Report and staff for O6/GS-15 signature, and the signed report will be submitted to USAREUR-AF G6 Cybersecurity Division for review. User accounts will remain disabled until adjudication is complete, upon which time the supervisor(s) and Director will be notified of incident resolution via email.

g. High- risk, high- impact violations including repeat CPV offenses, NDCIs, offenders with privileged access, and offenders with security clearance (T3 or T5) will be reported to the USAG Bavaria S-3/5 Protection Branch Security Manager and require O7/SES signature on AE Form 25-2B. The offender may be subjected to further adverse administrative actions in accordance with AR 25-2.