Your Security POCs for USAG Bavaria - Grafenwoehr:

Security Manager, 475-8121
Security Specialist, 475-8828
Security Specialist, 475-7138
References

- DoD Directive 5200.1 (Volumes 1-4) Information Security Program
- AR 380-5 DA Information Security Program
- USAREUR/AE Supplements
- Commander’s Guide To Incident Reporting
- USAG Bavaria Computer Incident Handling Pamphlet
Information Security

1. Classified Information
   Levels & definitions

2. Access
   Clearance + Nondisclosure Agreement + Need to Know

3. Violations & Reporting Procedures
   It is EVERYONE’S responsibility to safeguard information & report violations
What is classified information?

Official government information that has been determined to require protection, and has been so designated

Confidential – unauthorized disclosure will cause damage to our national security

Secret – unauthorized disclosure will cause serious damage to our national security

Top Secret – unauthorized disclosure will cause exceptionally grave damage to our national security
Recognizing Classified Documents

Classified material that has been removed from storage must have one of these coversheets attached.

SF 705  CONFIDENTIAL

SF 704  SECRET

SF 703  TOP SECRET
Recognizing Classified Information

• Physically marking classified information serves to warn and inform holders of the degree of protection required.

  • Overall classification & Page markings
    - Top Secret
    - Secret
    - Confidential

  • Portion (paragraph) markings
    - (TS), (S), (C) & (U)

  • Declassification instructions
    - Derived From, Date of Source, and Declassify On

Classified By: John Smith, Ops NCO
Derived from: OPORD209-X
Date of Source: 1 Jan 2007
Declassify on: 20171015

Classification markings are for training purposes only
Recognizing Classified Media

Always indicate highest Classification contained on the media:

- SF 710 (Unclassified label – Green)
- SF 708 (Confidential label – Blue)
- SF 707 (Secret label – Red)
- SF 706 (Top Secret label – Orange)
Access to Classified Information

In order to be granted access to classified information, you must have:

✓ Appropriate security clearance eligibility
✓ Nondisclosure Agreement (NDA)
✓ A need-to-know

Never share classified information in your possession with anyone who does not have these three things!
All DA personnel have the responsibility to safeguard national security information.

All DA personnel will report security violations.
Security Violations

• A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not it leads to a compromise of classified information.

• Individuals who commit security violations may be reported in JPAS (incident/derogatory report).

• In some cases, security violations may result in a revocation of security clearance, UCMJ or other civil/criminal action.
Security Violations

If you find classified material left unattended (for example, in a rest room or on a desk), it is your responsibility to ensure that the material is properly protected.

1. **Safeguard** the information immediately, even if you don’t have a clearance.

2. **Contact** your Security Manager or S2 immediately.
End of the Day Security Check

Check the entire work area for classified and sensitive materials

Check the container to ensure it is locked
  - SF 702 required for all “Safes”

Record checks on SF 701 (Activity Security Checklist)
  - Mandatory for Secure/Classified Storage Areas
  - Recommended for offices with Privacy Act, FOUO, or Personally Identifiable Information (PII)
You can’t take it with you.

Classified material is not personal property!
Incident Reporting is Everyone’s Responsibility
Contact your Security Manager, S-2 or the Garrison Security Office

USAG Bavaria Security Office
Security Manager  475-8121
Security Specialist  475-8828
Security Specialist  475-7138