



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND
U.S. ARMY GARRISON ANSBACH
UNIT #28614
APO AE 09177-8614

IMAN-ZA

12 December 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Franconian Military Community Installation Access Policy

1. This policy letter will remain in effect until superseded or rescinded.
2. Scope: This policy letter is punitive in nature, and applicable to all military personnel, DA civilians, local national employees, family members, contractors and guests assigned, attached, TDY, conducting business, visiting or training in the Franconian Military Community (FMC), which is defined as USAG Ansbach, USAG Bamberg, and USAG Schweinfurt. Individuals subject to the Uniform Code of Military Justice (UCMJ) who violate this policy are subject to administrative or judicial actions under Article 92, UCMJ. Individuals not subject to the UCMJ are subject to administrative or judicial actions in accordance with applicable federal, state and local laws.
3. References:
 - a. Army Regulation 27-10, Military Justice
 - b. Army Regulation 190-22, Search and Seizure
 - c. Army Regulation 190-56, The Army Civilian Police and Security Officer Program
 - d. Army in Europe Regulation 190-13, The USAREUR Physical Security Program
 - e. Army in Europe Regulation 190-16, Installation Access Control
 - f. Army in Europe Regulation 525-13, Antiterrorism/Force Protection
 - g. Army in Europe Regulation 600-700, Identification Cards and Individual Logistical Support
 - h. Army in Europe Regulation 27-9, Misconduct by Civilians
 - i. USAREUR Regulation 604-1, Foreign National Screening Program
 - j. Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control"

4. Commander's intent: The Global War on Terrorism (GWOT) requires our communities to be vigilant and prepared to face an adversary that seeks to gain insight to our operations. Installation access control measures are in place to not only combat this threat, but also to ensure the safety and security of those who live and work in our communities. This policy outlines the requirements and procedures for installation access control within the FMC. Changes in the baseline force protection posture within FMC may warrant changes to this policy to ensure the security of our installations. This policy does not apply to restricted areas governed by other regulations.

5. Installation access within FMC will be strictly enforced. This policy will not be supplemented without approval of the FMC Commander. Army in Europe Regulation (AER) 190-16, Installation Access Control is the policy and procedures for the installation access control to U.S. Forces installation in the European theater. This policy is intended to supplement AER 190-16 with local procedures and guidelines for areas not specifically covered in the regulation. The procedures of this policy will:

a. Facilitate the compliance with force protection condition (FPCON) measures related to access control.

b. Facilitate the identification of individuals who do not have a need or are not entitled to access our communities.

c. Incorporate the FMC Installation Access Control System (IACS) into this policy.

6. Responsibilities:

a. The USAG Ansbach Directorate of Emergency Services (DES) will:

(1) Serve as the FMC access control proponent.

(2) Conduct staff assistance visits and command inspections for IACS registration and installation pass procedures compliance.

(3) Ensure all Installation Access Control Offices (IACOs) comply with regulatory requirements.

b. School buses: All school bus drivers must have a valid installation pass for access to the installation. School bus drivers will vouch for all students on the bus. Drivers that do not have a valid installation pass must be escorted to and from the pickup/drop-off location on the installation by a DoDEA contract bus representative.

c. Tour buses: For unaccompanied access, the sponsor of the tour will provide bus driver and vehicle information prior to arrival. The bus driver, upon initial entry to an installation (first pick-up), will produce a manifest, which lists the time, date, and location of personnel pickup for

IMAN-ZA

SUBJECT: Franconian Military Community Installation Access Policy

an authorized tour. When the tour bus returns, a DoD ID card holding tour manager may vouch for the occupants.

d. Government shuttle buses: All shuttle bus drivers must have a valid installation pass for access to the installation. Shuttle bus drivers may vouch for all occupants on the bus.

e. VIP vehicles: For visiting VIP's, the USAG protocol office will coordinate the access and have a representative at the ACP to assist the guards in coordinating the access. In the absence of a protocol officer or FMC representative the driver will present his/her DoD ID card or valid installation pass for access to the installation. Passengers will not be required to produce identification. The vehicle will not be searched.

f. Military convoys: The convoy commander will remain at the access control point and vouch for vehicles/personnel within the convoy.

g. Military formations, to include physical training (five or more personnel): One person with a DoD ID card can vouch for the rest of the individuals within the main body of the formation.

7. Franconian Military Community member's guest(s):

a. DOD ID card holders and installation pass holders with sign-in privileges may sign in up to four individuals at the access control point. The individual being signed in will present a valid form of identification (passport or national ID) at the access control point. Guests will be escorted at all times by a trusted agent (ID card or installation pass holder) to include returning to the access control point to sign out. Contractors do not have to be signed out by the same person that signed them in, but the escort must be a trusted agent.

b. Per the FMC Commander, guests who are signed in are limited to a 24 hour period. Family members who are arriving over the weekend/holiday may get an exception-to-policy to allow time for the IACS office to open and receive an installation pass. For other situations, if the visit is to exceed 24 hours then both the sponsor and guest(s) will report to the ACP where the sign-in occurred and the sponsor will resign-in their guest(s). Violators of the 24 hour sign-in period may be subject to administrative or judicial actions under the UCMJ or Civilian Misconduct Action Authority for Article 92, Failure to Obey a Lawful Order. Failure of the sponsor to return to the ACP and sign out their guest will result in the loss of sign-in privileges:

- (1) For the first offense the sponsor will lose sign-in privileges for 30 days.
- (2) For the second offense the sponsor will lose sign-in privileges for 60 days.
- (3) For the third offense the sponsor's sign-in privileges will be permanently revoked.

c. Per the FMC Commander, the clarification of the policies for sign-in of underage persons/minors is to ensure that members of the community, family or friends, are not unduly denied access to the installation during a legitimate visit.

(1) A minor is any person under the age of 18. Children under the age of 10 do not need to provide ID documentation to be allowed access to the installation when accompanied by an ID card holder. An individual under the age of 18 can be signed onto the installation if:

(a) The minor is accompanied by a verifiable legal guardian who gives their consent. Verifiable means that the adult in charge of the minor can reasonably demonstrate their authority to give consent. For example, the names match on the national ID or the address is the same on identification documents or paperwork.

(b) The sponsor (the ID card holder signing in the minor) is accompanied by a spouse or a family member as defined below.

(2) For the purpose of this guidance, the definition of a family member is limited to a son, daughter, parents, brothers, sisters, mother-in-law, father-in-law, brothers-in-law, sisters-in-law, grandparents, and grandparents-in-law.

d. The FMC Garrison Commanders or designated representative may authorize personnel with Trusted Traveler privileges IAW DTM 09-012, reference j, attachment 3, paragraph 3.e.1.

The Trusted Traveler procedure allows a uniformed service member or Government employee with a valid CAC, a military retiree (with a valid DoD identification credential), or an adult dependent (with a valid DoD identification credential) to present their identification token for verification while simultaneously vouching for any vehicle occupants. The number of personnel a Trusted Traveler is allowed to vouch for and/or sponsor at any one time will be determined by the local installation commander or their designated representative.

8. Access Control Point (ACP) procedures:

a. Search authorization: Any vehicle or person attempting to access a FMC installation is subject to search IAW AR 190-22 and USAREUR Supplement 1 to AR 190-22.

b. Forgotten ID Cards: ACP guards will verify that the individual is authorized access to the installation by performing a manual look-up.

c. Confiscation:

(1) All DoD ID cards and installation passes that are expired will be confiscated by ACP guards or Military Police. ID cards or installation passes that are mutilated have illegible identification data or an unrecognizable photo will also be confiscated if the officers cannot positively verify that the individual matches the picture on the ID.

IMAN-ZA

SUBJECT: Franconian Military Community Installation Access Policy

(2) An individual who has their ID card or installation pass confiscated will be issued an AE Form 190-16B. The AE Form 190-16B is not an access document.

(3) Within 24 hours, confiscated installation passes cards will be sent to the IACO and confiscated DoD ID cards will be sent to the DEERS ID card office by the DES.

(4) Individuals who have their pass or ID card confiscated must be signed in as a visitor until a new pass or ID card is issued.

(5) Military Police will be notified when an individual fails to comply with any directives or orders, or objects to surrendering an expired ID card or installation pass.

9. Installation Passes: The USAG-Ansbach DES is the FMC staff proponent for installation passes and works with ICW and the (DPTMS) security manager to ensure this program is managed under the guidelines of the Local National Screening Program (LNSP). In regards to the categories listed in AER 190-16, Local USAG Commanders may request additional background checks for the following categories:

a. Official Guest Category – Police Good Conduct Certificate, AE Form 604-1B and entered into the Local National Screening Program.

b. Visitor Category (Residing in Europe) – AE Form 604-1B and entered into the Local National Screening Program.

c. Other Category – Police Good Conduct Certificate, AE Form 604-1B and entered into the Local National Screening Program.

d. Delivery Drivers – Installation Passes should be initially issued for 6 months and only when accompanied by the service owner. Drivers who have established themselves in the community through years of service without incident may receive renewals for 1 year. Owners must supply the IACS office copies of the business license and food preparation health certificate. Taxi drivers may be issued a pass for two years.

e. Sponsors for installation passes will:

(1) Ensure that privileges for installation passes are limited.

(2) Installation pass holders granted sign-in privileges for official business only, are limited to four persons with their vehicles. Persons granted sign-in authority should either be in a supervisory position or have an official need to ensure mission accomplishment (i.e. COR, project manager, etc.).

(3) Individuals who abuse their installation pass privileges (i.e., use their installation pass as a means to access the installation for other purposes than the intent of the installation pass)

IMAN-ZA

SUBJECT: Franconian Military Community Installation Access Policy

will have their installation pass revoked. ID cards and installation pass holders who abuse the sign-in privilege (i.e., the guest is unescorted, the guest does not sign-out) may have their sign-in privileges revoked.

10. The proponent for this policy is the Director of Emergency Services at DSN 467-3855.

DISTRIBUTION:

A