CG POLICY	Number: 1
SUBJECT: Open Door Policy	Date: 10 AUG 2007

1. My open door policy is as follows:

a. Individuals should try to resolve problems through their chain of command, Equal Employment Opportunity, Equal Opportunity, Inspector General, appropriate union, or Management/Employee Relations channels. Normally, issues pending before these authorities, and those matters pending criminal investigation, disposition under the Uniform Code of Military Justice, adverse administrative action or resolution by Military Intelligence authorities should be addressed through the above channels before they are a proper subject for open door consideration.

b. Once the particular process involved permits, I will consider speaking to or seeing anyone who feels their problem has not been resolved satisfactorily or in accordance with law or regulation. It is helpful if background information pertaining to the problem and a specific written statement of the desired action is provided for my consideration.

c. I strongly encourage enlisted Soldiers to consult with the HQ USAAC Command Sergeant Major prior to requesting to see me.

2. Military and civilian personnel will not, unless legal considerations prevent, be prohibited or discouraged from making appointments to see me consistent with this policy.

3. To request an appointment on my Open Door Policy, please contact my office at (757) 788-2207 (DSN 680-2207).

4. Commanders and their staff directors will establish an open door policy appropriate to the nature of their organization. Further, they will ensure open door policies are publicized.

5. A copy of this policy will be posted on all bulletin boards.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 2
SUBJECT: Safety	Date: 10 AUG 2007

1. The safety and well being of all personnel and their families are vitally important and affect our ability to succeed as an organization.

2. Safety awareness and enforcement are important parts of successful operations. A safe environment is a valuable mission enhancer and conserves critical mission resources. We must integrate safety into all activities, working to eliminate accidents, injuries and fatalities.

3. Safety is everyone's responsibility. A commitment to safety is essential to fostering a command climate where all members can contribute towards accomplishment of our mission. I will lead the effort personally and expect every Soldier and civilian employee in this command to make safety a priority.

4. Commanders and supervisors must demonstrate positive leadership in observing and enforcing safety standards, implementing risk management and improving safety and occupational health in areas under their control. Commanders and supervisors are accountable for ensuring their people know the hazards of the workplace and receive appropriate training on how to work safely. Report health and safety hazards to the TRADOC Safety Office immediately.

5. You are irreplaceable. Safety is everyone's responsibility.

Let's all work to
be Army Strong
as Army Safe!

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 3
SUBJECT: Suicide Prevention	**Date:** 10 AUG 2007

1. The Command is not immune to the tragedy of suicide. Leaders should know their people; know their units; foster an organizational climate of mutual support; and help members build a community where no Soldier, employee, or Family member is left alone or hopeless when suffering debilitating stress.

2. The performance of even our best members can be impacted at times by life's difficulties. Every member of the command must watch for signs which may indicate someone is contemplating suicide:

a. **VERBAL SIGNS:** "You'd be better off without me," "I wish I were dead," "I have no future; it's hopeless and I have ruined my life," "What's the sense; my problems will be over soon."

b. **PLANS FOR DEATH:** Knows how and when they may kill themselves and has the means (access to lethal weapons); gives away prized possessions.

c. **MENTAL WELL BEING:** Mental health issues, depression, unusual sadness, sense of hopelessness, increased anxiety or total loss of interest, and special stressors (marriage, divorce, loss of significant other, special family needs, legal, financial and medical problems, death of someone close).

d. **BEHAVIORAL CHANGES:** Sleeplessness, weight loss, increased risk-taking behavior, increased alcohol use, irritability, loss of appetite.

e. **HISTORY:** Previous attempts or a family history of suicide.

3. Signs of emotional distress and potential suicide require the observer to act. It takes personal courage to inform your commander or supervisor about your "Battle Buddy" or the pain you are suffering yourself; do not risk regrets later because you do not want to get involved or are too busy to be observant enough to recognize a suicidal signal before it is too late.

4. Our goal is to help every individual recognize the warning signs for suicide in themselves and others. I challenge every leader and manager to erase the stigma attached to seeking mental health services. Our message is that seeking help is a sign of personal courage--a key Army value.

5. Lastly, many resources exist to help with this critical problem: mental health providers, Chaplains, Army Community Service, Red Cross, and the entire USAAC family who must consider themselves as valuable contributors to the solution.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 4
SUBJECT: Sponsorship Program	Date: 10 AUG 2007

1. The USAAC Sponsorship Program assists Soldiers and civilian employees, and their Families during the reassignment process. It also improves unit cohesion and readiness by decreasing distractions that hamper personal performance and mission accomplishment.

2. Newly assigned personnel and their Families will develop their first impressions of their unit and the installation based on how well they are received. Sponsors make first and lasting impressions, and commanders must ensure that these impressions are positive. Sponsorship is more than sharing information. Good sponsors reach out to their new arrivals to ensure they feel welcome and understand that they are important additions to their new organizations. The result of their efforts will not only affect how new personnel view their new assignments, but also affect performance, morale, retention and ultimately readiness.

3. Commanders will ensure every new arrival is assigned a sponsor, and must ensure that sponsorship welcome packets are available through our many ways of passing information to include use of the web.

4. Upon identification of a gain, a welcome letter will be sent from the appropriate commander. If the first notification of a gain is the Soldier's arrival, "Reactive sponsors" will be appointed. In every case, commanders will ensure that appointed sponsors be provided the time and resources necessary to carry out the task from start to finish. Commanders should attempt to match new arrivals and sponsors by grade, experience level and marital status.

5. A properly managed sponsorship program sets the conditions for a positive command climate. Sponsored personnel benefit by learning how to avoid and prevent problems before they or their Families experience hardship; leaders benefit by gaining personnel who feel welcome and understand their contribution to the organization from the onset of their assignment. Effective sponsorship programs are the first step in achieving this goal and our readiness multipliers.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 5
SUBJECT: Delegation of Authority to Downgrade Awards	**Date:** 10 AUG 2007

1. References:

a. AR 600-8-200, Military Awards.

b. USAAC Regulation 600-2, Awards and Special Recognition Programs.

2. Authority is delegated to the Commanders of U.S. Army Training Center-Fort Jackson, U.S. Army Cadet Command, U.S. Army Recruiting Command, and U.S. Army Accessions Support Brigade to disapprove and downgrade award recommendations for U.S. Army personnel assigned or attached to their command provided the commander has the authority to approve the next lower level award.

3. The commanders listed above are also granted permission to further delegate disapproval authority to their subordinate commanders as long as it is done IAW the provisions of AR 600-8-22, para 3-5d.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 6
SUBJECT: Equal Opportunity/Equal Employment Opportunity (EO/EEO) Program	**Date:** 10 AUG 2007

1. I am totally committed to EO and EEO concepts, policies and objectives which ensure equal treatment without regard to race, color, religion, age, gender, national origin or physical or mental disability. I expect each member of this command to be equally committed to the concepts, policies and objectives.

2. EO and EEO are inherent parts of all personnel management policies, procedures, practices and actions that affect employment, assignment, promotion, training and professional development. These programs are equally applicable when recognizing, rewarding, disciplining, and providing proper working conditions for our employees.

3. Every member of this command will have an opportunity to achieve his or her full potential based on his or her abilities, merits and qualifications. Our mission requires the essential elements of mutual trust and unit cohesion. These essential elements can only be achieved when individuals are confident that fair treatment and respect for their capabilities exist. Commanders, supervisors and all employees of USAAC must realize that equal treatment of all Soldiers and employees is an integral part of accomplishing the command's mission.

4. Discriminatory practices are unacceptable in this command. Allegations of discrimination will be dealt with expeditiously, with management's personal involvement in the resolution of the allegations. When discrimination occurs, appropriate disciplinary action will be taken.

5. A copy of this memorandum will be displayed permanently on official bulletin boards. Commanders will ensure subordinate supervisor and employees are informed of this policy.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 7
SUBJECT: Equal Opportunity/Equal Employment Opportunity (EO/EEO) and Sexual Harassment Complaint Procedures	**Date:** 10 AUG 2007

1. All federal employees have the right to file a complaint if they believe they have been discriminated against based on their race, color, gender, national origin or religion. They also have the right to file a sexual harassment complaint if they feel they were sexually harassed.

2. Commanders at all levels will create an environment that enables our Soldiers and employees to file a complaint without fear of reprisal.

3. Although not always possible, Soldiers and employees should attempt to resolve complaints informally by confronting an alleged offender informing him or her that the behavior is offensive and demand that it stop. If this action does not resolve the matter, I urge addressing the complaint through the chain of command or supervisor.

4. Soldiers should contact the TRADOC EO advisor or AAC EO representative. Civilian employees should contact Headquarters, Fort Monroe EEO representative.

5. A copy of this policy will be posted on all bulletin boards.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 8
SUBJECT: Sexual Harassment	Date: 10 AUG 2007

1. USAAC is totally committed to the Army's policy for the prevention of sexual harassment, and I expect all Soldiers and civilian employees to support the policy as well. I will not condone or tolerate anyone violating the Army's sexual harassment policy.

2. Sexual harassment is defined by the Equal Employment Opportunity Commission as unwelcome sexual advances, request for sexual favors, and other verbal or physical conduct of a sexual nature. Additionally, anyone in a supervisory or command position who engages in or condones implicit or explicit sexual behavior engages in sexual harassment.

3. Training is essential in eliminating sexual harassment. It is a Department of the Army requirement that all civilian supervisors must take the basic 4-hour Prevention of Sexual Harassment (POSH) course. This applies to all newly appointed or existing supervisors and is a one-time requirement. New employees are also required to attend basic POSH. The Army further requires that all supervisors and employees attend refresher POSH training biennially. Semi-annual training in the prevention of sexual harassment is mandatory for all Soldiers.

4. Preventing sexual harassment is everyone's responsibility, regardless of rank or position. Any action that jeopardizes the public trust and confidence in our organization has an adverse effect on our ability to accomplish our mission.

5. A copy of this memorandum will be displayed on all official bulletin boards.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 9
SUBJECT: Sexual Assault Prevention and Response (SAPR) Program	**Date:** 10 AUG 2007

1. Sexual assault is intentional sexual contact characterized by use of force, physical threat or abuse of authority, or when the victim does not or cannot consent. Sexual assault includes rape, nonconsensual sodomy (oral or anal), indecent assault (unwanted, inappropriate sexual contact or fondling), or attempts to commit these acts. Sexual assault is a crime not limited by gender, spousal relationship or age of victim.

2. Sexual assault is not only counter to our Army Values and Warrior Ethos, but it is also an egregious crime that must receive the personal awareness of everyone. The Army's SAPR program reinforces its commitment to eliminate incidents of sexual assault through a comprehensive policy that centers on awareness and prevention, training and education, victim advocacy, response, reporting, and accountability.

3. In this command we will:

a. Take all sexual assault allegations seriously.

b. Thoroughly investigate the facts surrounding any allegation.

c. Hold those who commit sexual assault offenses accountable.

d. Handle all information regarding sexual assault with appropriate sensitivity.

e. Treat victims with dignity, fairness, and respect.

f. Provide confidential avenues for reporting.

4. It is the standard in this command that all Soldiers and DA civilian employees be trained on sexual assault risk reduction techniques as well as methods for reporting an incident should it ever happen. The chain of command, as well as health care professionals and criminal investigators, are in place to help. Should a victim of sexual assault desire to receive medical care, counseling, and victim advocacy without triggering the investigative process/chain of command involvement, that individual has the ability to confidentially report the assault using restricted reporting procedures.

5. All DoD installations are required to have sexual assault victim advocacy programs with fully trained Sexual Assault Response Coordinators (SARC). Specially trained victim advocates are available to assist and advise victims. Should an assault occur, victims should immediately contact their nearest SARC.

a. On Fort Monroe the SARC may be reached by calling (757) 387-0266

b. On Fort Knox, the SARC may be reach by calling (270) 352-8185.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 10
SUBJECT: Use of Government Information Technology (IT) Resources and Systems	**Date:** 10 AUG 2007

1. Proper use of government resources must be a priority for everyone in this command. I expect commanders, staff directors, and all other members of this command to ensure proper use of these valuable resources.

2. IT Resources and Systems may be defined as all communications systems (telephone, facsimile, e-mail, LAN/WAN, Internet/Intranet, and other communications circuits), automated systems (computers and their peripheral devices), visual information systems (projectors, cameras, sound systems, VTC systems) and records management equipment (photocopier, micrographics equipment, optical storage systems). The rules are clear, obvious, and easy to apply in most cases: government property and IT systems are furnished to employees for the conduct of official government business. Even under today's more relaxed guidelines, these resources are intended to be used only for official business and other *properly authorized* purposes. Authorized purposes may include personal use as permitted by the first supervisor who is a commissioned officer or a civilian above GS/GM-11 in the chain of command or supervision. Personal use, which is authorized by these commanders or supervisors, must be within the following parameters:

a. Use must generally be during non-duty hours (i.e., before or after work hours or during lunch or other authorized breaks).

b. Use must generally be infrequent and relatively short in duration.

c. Serve legitimate purposes such as telephonic or e-mail communications most reasonably made from your normal workplace, such as checking in with your spouse or children, making medical, home and automobile repair and similar appointments or making a bank or other financial transaction which might otherwise take an employee away from the work location.

d. Must impose no significant additional costs to the government or overburden the IT system.

e. Must not deny IT services to any other government employee accomplishing assigned missions (telephone lines, limited internet accesses, etc).

f. Be properly authorized by competent authority. Supervisors may revoke this authorization if it is abused.

3. In the past, blatant and obvious abuses have been noted in the use of some government IT resources such as computers, software, internet access and telephones. While some abuse may be due to the process of "getting acquainted" with emerging or new technologies, some rules are nonetheless perfectly clear and must be observed by all personnel:

a. Absolutely no attempts to find, view, obtain or distribute sexually explicit material.

b. No use of personal Home Pages on government IT systems. Only official USAAC e-mail accounts will be used for official e-mail.

c. Official e-mail is provided to support the mission. E-mail should be spell checked, be in good taste and, with exceptions previously mentioned, only for official business, whether internal or sent through the internet.

(1) Whenever possible, group e-mails should be coordinated with system administrators of the target mail systems to avoid reactionary closing of their systems to our message traffic.

(2) Group e-mails will not be made of "chain" messages, unofficial letters or memoranda that could be perceived by recipients as having official Army/USAAC sanction and which would adversely reflect on the Army or would appear to be incompatible with public service.

d. No advertising, soliciting or selling for a private business or as an agent of a commercial business using government IT systems. Personal items may only be solicited or sold on authorized bulletin boards.

e. No use of government-procured software outside the manufacturer's license.

f. No use of personal software on government computers without Director, Information Support Activity authorization.

g. No use of personal computers or hardware in the place of duty to handle official business.

h. No use of computer games on USAAC automation equipment, with the exception of the Army Marketing Games developed to encourage individuals to talk with Army recruiters.

4. The above rules and regulations are punitive; failure to abide by their clear guidance may subject members of the command (whether military or civilian) to disciplinary and/or adverse actions. All USAAC personnel must refrain from conduct involving government resources that is wrong, which violates clear regulatory policy and which could harm the command and/or the Army as an unintended consequence of thoughtless action.

5. You should be aware that any use of government IT services is with the understanding that such use is generally not secure, not anonymous and serves as consent to monitoring.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 11
SUBJECT: Use of Government Travel Card/ Split Disbursement	**Date:** 10 AUG 2007

1. The Government Travel Card (hereinafter called "card") is for use by Soldiers and government civilians to pay for reimbursable expenses and incidental non-reimbursable expenses associated with official travel. The card is not to be used for personal, family or household purposes. No person other than the cardholder is permitted to use the card for any reason. Misuse of the card may subject offenders to adverse disciplinary action.

2. Cardholders are responsible for payment in full of the undisputed amounts due in the monthly billing statement. The card is not a revolving credit line; cardholders may not make a minimum payment and carry a balance on their account. Cardholders are considered delinquent when their account balance is not paid within 30 days after the due date. Failing to file a travel voucher, or not receiving a settlement does not relieve the cardholder of the requirement to pay the bill when due. If the account is 60 days past due, the card will be suspended. At 120 days past due, the card will be cancelled.

3. Soldiers are required to manage their personal affairs satisfactorily and pay their debts promptly, including their Government Travel Card debt. Soldiers who are delinquent or make unauthorized purchases will be counseled concerning proper use of the card and their obligation to pay just debts. At a minimum, counseling for delinquent Soldiers should include setting up a payment plan and advising the Soldier of the possible disciplinary action that may result from the continued failure to pay his or her just debts. For additional guidance, refer to AR 600-15, Indebtedness of Military Personnel, chapter 3, paragraph 1-5.

4. It is imperative that travel cards are paid in full each month. To ensure cards are paid promptly and delinquency rates decrease, all USAAC travelers are required to use split disbursement. Travelers will annotate in block 1 of the DD 1351-2 a specific dollar amount to be sent to their travel card. Within 72 hours of disbursement a payment will be received by the government travel contractor. The difference will be sent via electronic funds transfer to the traveler's personal account.

5. Let's work to eliminate delinquencies.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 12
SUBJECT: Timely Completion of Military Evaluation Reports	**Date:** 10 AUG 2007

1. Timely and constructive counseling of our subordinate's duty performance is one of our most important duties as leaders. A material part of that duty is the prompt completion of personnel evaluation reports. Reports must be forwarded to reach HQDA IAW the requirements of AR 623-105. Senior raters have the responsibility of ensuring reports are received at HQDA in the desired sequence to manifest their intent.

2. Whenever possible, I expect personnel evaluation reports to be finalized and handed to the rated individual the first day following the "Thru Date" of the report. If I am in the rating chain, that means the report shell needs to be on my desk not later than 14 days prior to the end of the evaluation period.

3. I want to reemphasize the purpose of evaluation reports: (1) to instill/reinforce Army values, (2) to improve duty performance through increased emphasis on performance counseling, and (3) to provide DA centralized selection boards and career managers with timely and accurate information to ensure those selected for special assignments, schooling, and promotion are the best qualified. As leaders, we play a central role in the effectiveness of the system, and the timely completion of reports deserves your personal attention.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 13
SUBJECT: Timely Completion of Civilian Evaluation Reports	**Date:** 10 AUG 2007

1. Performance management is an inherent responsibility of all those in positions of leadership. Requiring annual written individual performance evaluations provide supervisors and managers with tools for the systematic assessment of performance which, in turn, allows them to make sound plans and decisions. These evaluations foster a continuing basis for effective supervisor-subordinate partnerships in pursuit of common goals.

2. The civilian performance evaluation is designed to improve performance.

a. Communicating organizational goals and priorities, and Army Values and ethics to employees.

b. Establishing individual expectations for performance that reflect organizational goals and priorities.

c. Facilitating frequent discussion among the Ratee and the rating chain about performance, expectations, professional development and DA values and ethics.

d. Providing an environment where all understand that they are important members of the Army Team.

3. I expect each civilian Ratee to provide their support form to their Rater by the end of their rating period. In turn, each Rater must prepare their appraisal of the civilian Ratee and, where applicable, forward to the Senior Rater within 21 days of the end of the rating period. The Rater, or, where applicable, the Senior Rater should complete the appraisal, provide copy to Ratee and forward signed copies to the Resource and Logistics Management Directorate (RLM) within 30 days of the end of the rating period. RLM will forward properly prepared reports to the South Central Civilian Personnel Operations Center for processing.

4. In addition, I expect Ratees and their rating chains to have written performance plans in place within 30 days from the beginning of each rating period. This plan should represent a joint effort of Ratees and their rating chain. These plans must be reviewed and approved by the rating chain at least at the beginning of the rating period and any other time that expectations change significantly.

5. The Individual Development Plan (IDP) is a key enabler to better manage professional development and prepare our career members for positions of greater responsibility and authority. I strongly encourage supervisors, managers and rated individuals to work in partnership to outline an IDP designed to reach career goals. It is imperative we provide everyone the encouragement, time and resources to succeed.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 14
SUBJECT: Civilian Incentive Awards Program	**Date:** 10 AUG 2007

1. References.

a. AR 672-20, Incentive Awards, 29 Jan 99.

b. TRADOC Supplement 1 to AR 672-20, Incentive Awards, 19 Jan 05.

c. AR 690-400, Chapter 4302, Total Army Performance Evaluation System, 16 Oct 98.

d. Memorandum of Instruction, subject: USAAC Civilian Incentive Awards Guidance, 12 May 05.

2. This policy establishes guidance for the Civilian Incentive Awards program in HQ USAAC organizations located at Fort Monroe, Fort Knox and Accessions Support Brigade (ASB). This program, comprised of both monetary and honorary awards, is designed to reward employees whose job performance and ideas benefit the Government, and whose contributions are substantially above normal job requirements or performance standards. Reference d provides detailed guidance on preparation and approval of awards. Managers and supervisors are responsible for endorsing and supporting this program on a continuing basis to reap the significant contributions that the program promotes, i.e., fostering mission accomplishment and encouraging high levels of performance and service.

3. This policy is effective throughout HQ USAAC and ASB to ensure consistency and integrity of our awards program. In addition to the Civilian Incentive Awards plan, nomination and approval procedures are supplemented by any applicable Labor Management Agreements negotiated with this command.

4. Ensure widest dissemination of this guidance. Each commander and director is accountable for ensuring its application.

5. This policy supersedes all other memoranda on this subject.

6. POC is Mr. Charles Wilson, Director, G-4/8, HQ USAAC, DSN 536-0709, (502) 626-0709 or email: Charles.Wilson2@usaac.army.mil.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 15
SUBJECT: Consideration of Others (CO2) Program	Date: 10 AUG 2007

1. Reference memorandum, HQ TRADOC (ATBO-BPE), 6 Jan 98, subject: CO2 Program.

2. Purpose. To establish the U.S. Army Accessions Command CO2 Program.

3. Policy/Procedures.

a. Inculcation of CO2 as a value for this command is centered on a comprehensive education program which involves all Army and civilian personnel assigned. The purpose of this program is to enhance trust, cohesion, and readiness by ensuring continual awareness of caring as an organizational imperative.

b. The CO2 Program is a commanders program which instills in all members of the command a belief and understanding in the Army's core values: Loyalty, Duty, Respect, Selfless Service, Honor, Integrity, and Personal Courage. We must build and maintain an Army where people do what is right, where we treat each other as we would want to be treated, and where everyone can truly be all they can be.

c. The heart of the CO2 Program is the small group session. Well organized meetings in small groups are the ideal forum for building trust and teamwork within the command. To make these meetings a success, special attention must be taken in identifying and training CO2 group facilitators.

d. On an annual basis, the model CO2 Program for all Army and civilian personnel should include the following:

(1) Senior Leader/Middle Manager training.

(2) All military and civilian personnel receive training annually.

(a) Quarterly sessions, small group discussion, with 15-25 personnel

(b) Instructed by trained facilitators, who have attended the small group instructor trainer course and a 2-day CO2 facilitator seminar

e. Leader involvement at all levels is the essential ingredient to a successful program. Equal Opportunity Advisors provide the Commander key staff support for implementation of this program. Training is required to be executed down to the lowest level.

4. Proponency. The proponent for this command policy is the TRADOC Equal Opportunity Office, (757) 788-5076.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

CG POLICY	Number: 16
SUBJECT: Guidance on Protecting Mobile/Portable Electronic Data Systems (PEDS) and Removable Media in USAAC	**Date:** 24 AUG 2007

1. References:

a. AR 25-2, Information Assurance, 14 NOV 03.

b. AR 380-5, Department of the Army Information Security Program, 29 SEP 00.

c. AR 735-5, Policies and Procedures for Property Accountability, 25 FEB 05.

d. Memorandum, Chief Information Officer (CIO)/G-6 (SAIS-GKP), 28 SEP 06, subject: Army Data-At-Rest (DAR) Protection Strategy.

e. Memorandum, OSD, 15 JUL 05, subject: Notifying Individuals When Identifying Information is Lost, Stolen or Compromised.

f Memorandum, TRADOC (ATCS), 31 OCT 06, subject: Guidance on Protecting DAR.

g. AR 25-55, Department of the Army Freedom of Information Act Program, 1 NOV 97.

2. Applicability: This policy applies to, and is binding on, all military and civilian personnel assigned, attached, detailed or on temporary duty with the U.S. Army Accessions Command (USAAC).

3. The failure to adequately protect portable computing devices and removable media continues to be the leading factor in the loss of sensitive Army data. These losses reduce the effectiveness of the command and put our mission in jeopardy. All USAAC activities shall ensure all mobile/portable electronic computing devices and removable/portable media containing sensitive data are protected.

4. Enforceability: Mobile/portable electronic devices (PEDs) include laptops, Blackberries, Treos and similar devices which may store sensitive data (e.g., Privacy Act, HIPPA, and Acquisition). Removable media includes items such as CDs, DVDs, floppy disks, thumb drives, flash memory, memory sticks, magnetic tape, other optical media, external or removable hard drives and other similar portable/mobile media devices containing sensitive data. Any such items that contain sensitive data are subject to this policy. Violation of paragraph five of this policy is punitive. Military personnel violating this policy may be subject to action under the Uniform Code of Military Justice and/or adverse administrative action. Civilian employees who violate this policy may also be subject to adverse action or discipline in accordance with applicable laws and regulations.

5. The following mandatory procedures shall apply to all government-owned or leased PEDS (devices) and removable/portable media containing sensitive data (media) within USAAC:

CG POLICY NUMBER: 16
SUBJECT: Guidance on Protecting Mobile/Portable Electronic Data Systems (PEDS) and Removable Media in the USAAC

a. When traveling with PEDS or portable media devices to any place outside the office (hotel, home, meeting site), the device or media must have all sensitive information in an encrypted form. The traveler must carry it/them on his or her person (whenever feasible) or always maintain positive physical and visual control of the device/media. When leaving an area and carrying the device/media is not practical, it must be locked in a reasonably secure container or placed under the control of a co-worker. For notebook computers, cable and lock mechanisms shall be used to secure the computer to a difficult-to-move object if the device may be exposed to theft. Kensington cable locks are available through supply channels and are available at Fort Knox.

b. While traveling by airplane or train, devices must not be checked with other baggage. The preferred method of security is for the traveler to hand carry the device onto the conveyance and carefully store and retrieve the device from the overhead bin or under the seat. The device must remain within the traveler's sight and within immediate reach at all times.

c. While traveling by POV or GOV, PEDS or portable media devices must not be left in the vehicle. The preferred method of security is for the traveler to hand carry the device and keep it in sight and within immediate reach at all times.

d. Neither PEDS nor portable media devices will be left unattended and unsecured in the workplace. When in the office, if the device is not under one's immediate control, lock the device in the office, secure it with a locking cable mechanism, or place the device in an appropriate container (such as a safe, lockable closet or lockable cabinet.)

e. No PEDS or portable media devices containing sensitive information will be used for travel or removed from a defense installation or government-controlled facility unless the following criteria are met:

(1) An Army approved encryption solution is loaded, active, and sensitive data is encrypted on the device.

(2) An USAAC Label 3 is affixed to the outside cover of the laptop computers so they will be visible for inspection, and a USAAC Label 2 will be used on the smaller portable devices, such as the Blackberry, thumb drives and other portable media. The labels will state that they comply with the Army data encryption standard and are authorized for travel. The labels are available through your normal publications and forms resupply channels who will order through the Supervisor of Publications and Forms, Information Services Division, Enterprise Services Branch, USAAC, Fort Knox, KY 40121, via DA Form 17, Requisition for Publications and Blank Forms.

(a) Recruiting Battalions will support their Battalion Headquarters, Companies, Stations, and Recruiters.

(b) Recruiting Brigades will support their Headquarters.

(c) ROTC Regions will support their Headquarters.

(d) ROTC Brigades will support their Brigade Headquarters and their Schools.

(3) Passwords will also be used on the Blackberry and other portable devices that are not Common Access Card (CAC) enabled:

f. All computer devices shall be hand receipted, PEDS and media approved for travel will be hand-receipted as personal issue equipment. An inventory for all computer devices and portable storage media shall be maintained and verified at least annually to ensure accountability. Liability for the loss or theft of computer devices shall be evaluated in accordance with this policy and AR 735-5. Failure to follow this policy, or other guidance on laptop security, may constitute negligence and subject the violator to personal financial liability.

g. Any government-owned or leased portable device or media used to store, or intended to store, sensitive data shall be subject to inspection.

h. Portable devices and media should, by default, not contain sensitive information or personally identifiable information (PII). It should only be stored by exception and when mission accomplishment necessitates its usage. If this information is stored on portable devices and media, it will be encrypted. Once sensitive information is no longer needed it should be deleted from the device or media.

i. All users will be trained in the protection of sensitive data and the use of USAAC approved encryption software. Users will also receive annual refresher training. Training materials are posted on the USAAC portal.

j. Should a device or media containing sensitive data be lost, stolen or destroyed, the user will immediately notify his or her chain of command (CoC) and the CIO designated Automation Support Officer or Information Management Officer (IMO). The CoC will immediately initiate a Serious Incident Report detailing the data involved and the circumstances of the loss. The loss will also be reported to the USAAC Privacy Officer by the CoC, who will contact:

(1) The U.S. Computer Emergency Readiness Team (US-CERT) within 1 hour.

(2) The DoD Component Privacy Office/point of contact within 24 hours.

(3) The DoD Privacy Office within 48 hours.

k. All portable devices containing or used with sensitive data shall use the CAC as the primary means of authentication. Blackberry and TREO devices are currently exempted from the CAC requirement due to poor reader performance, but they shall be configured to require the use of a password for access.

l. Personal (non-government owned) devices and media will not be used to store or transport government proprietary or sensitive data.

6. In addition to the mandatory procedures above, I expect commanders and supervisors to be vigilant and proactive. Physical security is the first line of defense. Commanders and supervisors must evaluate the risk and vulnerabilities of loss and theft and must take all reasonable measures necessary to ensure adequate safeguards are in place for all government-owned or leased mobile and portable computing equipment and devices, and removable and portable media containing sensitive data.

7. Although portions of this policy are punitive, commanders and supervisors are reminded to consider the full range of options for addressing misconduct and disposing the case at the lowest appropriate level consistent with the gravity of the misconduct.

8. Point of contact is G6-ISA Information Support Activity, Information Assurance, USAAC, Fort Knox, KY 40121.

BENJAMIN C. FREAKLEY
Lieutenant General, U.S. Army
Commanding

DEPARTMENT OF THE ARMY
COMMANDING GENERAL, UNITED STATES ARMY ACCESSIONS COMMAND/
DEPUTY COMMANDING GENERAL FOR INITIAL MILITARY TRAINING
90 INGALLS ROAD, BUILDING 100
FORT MONROE, VIRGINIA 23651-1065

REPLY TO
ATTENTION OF

ATAL-CG

20 JUL 2007

MEMORANDUM FOR RECORD

SUBJECT: CG USAAC Physical Training Policy Memorandum

1. Leaders are responsible for ensuring Soldiers under their command present a neat orderly appearance and conduct themselves professionally both on and off duty. To ensure good order and discipline, and to ensure our Soldiers present a professional appearance when conducting unit physical training (PT), the below policy is effective immediately.

2. The Army Improved Physical Fitness Uniform (IPFU) shall be the only clothing worn by Soldiers assigned to U.S. Army Accessions Command (including subordinate commands) who are participating in unit or individual fitness training during the hours of 0530-0800. Soldiers who are pregnant shall wear the IPFU until the uniform becomes too uncomfortable, at which time the wear of appropriate civilian workout attire is authorized.

3. Radios, walkmans, IPODs, blue tooth headsets, or other similar devices are not authorized for wear with the IPFU. Reflective vests or belts will be worn by individuals running or performing PT at night, during periods of low visibility, and in unit PT formations.

4. With the exception of a leader going out to check a unit's PT session, PT will be done in buddy teams.

Army Strong!

BENJAMIN C. FREARLEY
Lieutenant General, U.S. Army
Commanding