

CEPM-ZC (380-19)

~~20 January 1999~~

Feb 1995

MEMORANDUM FOR DIRECTORS, HQUSACE
CHIEFS, SEPARATE OFFICES
COMMANDERS, USACE COMMANDS

SUBJECT: Policy Statement on Use of Privately Owned Computer and/or Software

1. **Purpose.** This policy provides guidance on the responsibilities and liabilities of both the Corps and the user of a privately owned computer used off-site, ie. at home, for the employees convenience in performing official government duties.

2. **References.**

- a. AR 380-19, Automation Security, 1 Aug 90.
- b. AR 25-1, Army Information Resources Management Program, 18 Nov 88.
- c. Memorandum, HQUSACE, CEPM, 21 Apr 92, subject: Delegation of Authority for Accreditation of Automated Information Systems.
- d. 5 CFR, Part 551, Pay Administration under Fair Labor Standards Act.

3. **Understanding.**

a. Employees in grades GS-10 and below are **not authorized** to perform work at home, on a voluntary basis for the employee's convenience unless the employee is exempt under the Fair Labor Standards Act.

b. Employees in grades GS-11 and above and other exempt employees under the Fair Labor Standards Act may perform work, at home, on a voluntary basis. However, such employees may not receive credit hours, overtime, or other compensation for voluntary work performed at home.

c. The user of the privately owned computer will be designated the Information Systems Security Officer (ISSO), as outlined in AR 380-19 paragraph 1-6, d. (3), for that location.

d. The user (ISSO) of the privately owned computer will accomplish an accreditation document for the privately owned computer. The Designated accreditation Authority (DAA) for the privately owned computer will be the users commander or agency head as specified in AR 380-19, para 3-8 and AR 25-1, para 5-4. The DAA must be in the minimum rank of

lieutenant colonel, GM-14 or GS-14. The DAA must approve the accreditation of the privately owner computer, prior, to its use for Government work.

e. All Government related work processed on a privately owned or Government owned computer, regardless of the ownership of the computer, is the property of the United States Government.

f. In accordance with software license agreements, no United States Government owned software will be copied for use on a privately owned computer. No privately owned software will be copied for use on a Government owned computer. Privately owned software must be donated to the United States Government, before, it can be used on a Government owned computer. This software will become the property of the United States Government.

g. Classified information, data covered under the Privacy Act and unclassified sensitive data **will not be processed** on privately owned computers. Only unclassified, nonsensitive information may be processed on a privately owned computer in the home environment.

h. Privately owned computers will be checked for viruses prior to performing any government related work. All media used to transfer information from a privately owned computer, must be checked by the Corps/Army approved anti-virus software prior to down loading the information to a government owned computer.

4. Point of contact for this action is Mr. Thomas J. Aubin, (202) 272-8723.

FOR THE COMMANDER

THOMAS D. BLAIN
LTC, Military Police
Chief, Security and Law
Enforcement