DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE FLIGHT TEST CENTER (AFMC)
EDWARDS AIR FORCE BASE, CALIFORNIA

19 MAR 2003

MEMORANDUM FOR DISTRIBUTION A, B, C, D

FROM: AFFTC/IT

SUBJECT: Authorization to Utilize Personal Digital Assistants (PDAs)

References: (a) AFI 33-202, *Computer Security*
(b) AFI 33-202, Supplement 3
(c) AFI 33-201, *Communications Security*
(d) AFMAN 33-223, *Identification and Authentication*

1. PDAs have become increasingly popular as a way to conduct business and enhance productivity while away from and in the office. However, new technologies bring security risks. Because each and every one of us is responsible for the security of our network, this policy applies to all PDA users on Edwards AFB.

2. Individuals may use PDAs to process unclassified information from their desktop computers, to include the following: schedules, contact information, notes, e-mail, word-processing documents, spreadsheets, and presentations. Users may synchronize their PDAs with their desktop workstations. However, the desktop auto-synchronization feature must be disabled after each use. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account protected by an authorized network control center firewall.

3. Individuals may **NOT**:

a. Use PDAs to process or maintain classified information. There are currently no approved methods for cleaning or sanitizing classified information from these systems, therefore contaminated PDAs must be destroyed without cost reimbursement to the user or unit.

b. Use PDAs to process or maintain sensitive but unclassified (SBU) information. There are currently no approved methods for cleaning or sanitizing SBU information from these systems. Therefore contaminated PDAs must be destroyed without cost reimbursement to the user or unit.

c. Synchronize information across any Edwards network using wireless connections or connect PDAs with wireless features user-to-user. This practice creates unacceptable security risks to our network. Infrared ports will be disabled at all times, or covered with tape.

d. Connect or subscribe to commercial Internet service providers for official e-mail services.

e. Use PDAs in any environment where classified processing takes place (vaults, special access program areas, etc).

4. PDA users are strongly discouraged from using privately owned PDAs for official business. Personal PDAs must be approved for use on the network by the DAA: Justification must include descriptions of mission requirements and government availability, and rationale of how duty position will be enhanced. Each requestor must submit a PRIVATELY OWNED PDA USAGE STATEMENT (sample attached).

5. To further enhance information security measures, password protect all PDAs if technically feasible. If not, the user must maintain physical control of PDAs at all times to prevent unauthorized access. In addition, PDAs must be included in certification and accreditation packages; PDA operating systems must be compatible with the base network; and current anti-virus software must be installed on the PDA.

6. Failure to comply with this policy will result in loss of PDA privileges at Edwards AFB. If you have any questions please contact your Unit COMPUSEC Manager or the Base Information Assurance Office at 7-7819.

Shelley D. Christian

SHELLEY D. CHRISTIAN, Col, USAF
Director, Information Technology

Attachment:
Privately Owned PDA Usage Statement

PRIVATELY OWNED PDA USAGE STATEMENT

MEMORANDUM FOR AFFTC/IT

FROM: _____ Date: _____
(Rank, Name, Office Symbol)

Subject: Agreement to Use DAA-Approved Privately Owned Personal Digital Assistants (PDA) on the Air Force Enterprise Network

1. My signature below indicates I understand my privately owned PDA, a similar type PDA to the Edwards AFB-approved government PDAs, has been approved by the DAA for use. In addition to the requirements in AFI 33-202, *Computer Security*, I agree to all terms, actions, and conditions contained in this letter.

2. I will:
a. Register my PDA with my local equipment custodian for local accountability.
b. Maintain a password on my PDA according to the system security policy.
c. Use my PDA to process only unclassified, non-Privacy Act information.
d. Maintain the same anti-virus software, security standards, and other operational requirements as Edwards AFB government-issued PDAs. I understand I am responsible for covering the cost of any additional required hardware or software.
e. Not connect or subscribe to any commercial Internet service provider for official e-mail services.
f. Not synchronize information across the Air Force network using a wireless connection.
g. Physically disable any built-in wireless connectivity capability, including infrared.
h. Surrender my PDA (without cost reimbursement) if classified or sensitive but unclassified (SBU) information contaminates my PDA.
i. Report any software abnormalities to the unit Information System Security Officer.
j. Not load any software on my PDA without prior authorization.
k. Prior to leaving my current duty assignment, I will submit my personal PDA to Information Technology Customer Service for removal of all work related unclassified information.
l. Connect my PDA to the network or system as approved by the DAA, and no others.
m. Not connect my PDA to ANY Edwards network without the written approval of the DAA.
n. Consent to monitoring of my PDA, because it is connected to a system subject to monitoring.

3. I understand my PDA is subject to being audited at anytime to determine if my PDA contains classified information, SBU information, or information protected by the Privacy Act of 1974.

4. I understand that if my PDA contains SBU and/or classified information, the PDA will be destroyed and I waive any and all claims for cost reimbursement for damage or destruction.

5. I understand IT Customer Support will assist me with all PC-related problems but repair of my PDA is my responsibility.

6. I understand that, if at any time I fail to meet the conditions stated above, I will be required to remove my PDA from its connection within the AF protected enclave and submit it to the Information Technology Directorate for data sanitization.

7. I understand the Air Force does not assume any liability for my PDA, regardless of circumstance. I understand that all data entered on my PDA while performing government business becomes the property of the U.S. Government.

8. Device information:

a. Make & Model: _____
b. Serial number: _____
c. Operating system: _____
d. Installed software: _____
_____
_____

9. I can be contacted at _____.
(phone number/office symbol/e-mail address)

Signature: _____
Signature Block: _____
File:
1 - Maintain original copy with the ISSO
2 – Provide one copy to the individual's Unit COMPUSEC Manager
3 - Provide one copy to the individual