DEPARTMENT OF THE NAVY
NAVAL SURFACE WARFARE CENTER
DAM NECK
1922 REGULUS AVENUE
VIRGINIA BEACH, VIRGINIA 23461-2097

5239
CV
01 Jun 09

NAVSURFWARCEN DAM NECK POLICY LETTER 09-001

From: Commanding Officer

Subj: NAVAL SURFACE WARFARE CENTER (NSWC) DAM NECK POLICY ON PORTABLE ELECTRONIC DEVICES

Ref: (a) CNO Washington DC 272200Z Apr 01, Policy Update: Use of Portable Electronic Devices in the Navy
(b) COMNAVNETWARCOM Norfolk VA 180008Z Nov 08; ALCOM 167/08
(c) NAVSEA Policy Letter 12-02 of 15 Apr 02
(d) NSWC Dahlgren Policy Letter XD 001 of 6 Jun 06
(e) CO, CDSA Dam Neck Wireless Policy of 21 Aug 07

1. Purpose. To disseminate policy and guidance for the use of wireless communication solutions and Portable Electronic Devices (PEDs) including data-enabled cellular phones, two-way pagers, personal digital assistants (PDAs), removable storage devices, and handheld/laptop computers. References (a) through (d) provide additional references that prescribe higher-level PED policy for the entire Navy.

2. Scope. This policy applies to all NSWC Dam Neck (NSWCDN) military and civilian personnel, contractors, and visitors. All NSWCDN personnel, including contractors, shall adhere to the provisions of this policy. PEDs covered by this policy include, but are not limited to, the following:

a. Mobile computing devices (e.g., PDAs, handheld PCs, notebook PCs, Table PCs and laptops)

b. Mobile telephony devices (e.g., cell phones, two-way radios, satellite phones, Blackberry devices, etc.)

c. Two-way pagers, including those with e-mail capabilities (e.g., Blackberry devices)

d. Analog and digital cameras (still and video)

e. Analog and digital sound recorders

f. Portable storage media such as flash memory, memory sticks, thumb drives, multimedia cards, secure digital cards, micro-drive modules, portable Hard Drives, ZIP drives, ZIP disks, recordable CDs, DVDs, MP3 players, Ipods, digital picture frames and floppy diskettes.

3. Discussion. PEDs have become a ubiquitous tool for managing tasks, calendars, and staying in virtual contact with offices and families. The capabilities of these devices, and their potential use in or around areas where classified information may be discussed or processed, create new risks. Managers and users must maintain situational awareness when PEDs are permitted. PEDs and wireless technologies present a significant security risk when operating outside of prescribed guidelines.

4. Policy. The use of PEDs at NSWCDN shall be as follows:

a. Personally owned PEDs (except for voice-only cellular telephones) are not authorized for use at NSWCDN. This is to minimize the risk of inadvertent capture of controlled information by a personal PED, since the only approved method of "sanitizing" most PEDS is physical destruction. ALL PERSONALLY OWNED PEDs must be removed from NSWCDN. Individuals attempting to gain access to an NSWCDN building with a personally owned PED may have it confiscated during routine administrative inspections. Any unauthorized personally-owned PED discovered within any NSWCDN building will result in a security violation.

b. Per reference (b), government owned thumb drives are not authorized on any Navy computer. All government owned thumb drives will be turned in to the command Information Assurance Manager (IAM) for auditing, marking and storage.

c. All Government owned portable hard drives shall be registered in the command Computerized Asset System (CAS) program for property control, shall be scanned by the user monthly for malicious software and shall be registered with the command IAM. NMCI attached portable hard drives will be authorized on NMCI systems in accordance with Naval Network Warfare Command (NNWC) procedures. Portable hard drives are authorized for connection to a single computer only and not to transfer information between computers.

d. Government owned PEDs used at NSWCDN will adopt the following security measures:

(1) PEDs will not be connected to systems or networks processing government information without cognizant Designated Approving Authority (DAA) approval. For RDT&E systems, this means the NAVSEA RDT&E DAA, SEA OOI. For NMCI systems, this is the Naval Network Warfare Command (NNWC) operational DAA.

(2) PEDs will only synchronize with unclassified computers.

(3) PED wireless connectivity features (Bluetooth & Wi-Fi) shall not be active while inside NSWCDN facilities. Broadband wireless connectivity is authorized on NMCI issued Blackberry PDAs for voice communications and wireless data synchronization.

(4) PED wireless connectivity policy for NSWCDN (reference (e)) remains in effect.

e. No PEDs shall be brought into a Sensitive Compartmented Information Facility (SCIF) unless specifically authorized in writing by the Special Security Officer (SSO) or the Senior Intelligence Officer (SIO). No PEDS shall be brought into Open Secret Storage areas unless specifically authorized in writing by the Information Assurance Manager or the Physical Security Officer.

f. PEDs will not be used to store passwords, safe nor door combinations, or personal identification numbers (PINs). The authorized exception being the password keeper function on NMCI issued blackberry PDAs which shall hold password information for unclassified systems only.

g. All PEDs will use appropriate Data Encryption at Rest promulgated by higher authority.

h. All PEDs shall support the use of the DoD Common Access Card (CAC) for authentication, digital signatures and data encryption. All PDAs shall use CAC for such purposes no later than December 31, 2009.

i. All wireless data communication systems must be certified and accredited by the cognizant DAA. Pilot projects must implement appropriate security requirements and processes during the development of the system.

j. PEDs shall employ up-to-date anti-virus software signature files that are used to profile and identify viruses, worms, and malicious code. PEDs shall be configured with appropriate security settings prior to being issued to users. Passwords shall be a minimum of eight alphanumeric characters.

k. The possession or use of video or camera cellular phones and other recording reproduction or photographic devices are prohibited in any NSWCDN building except for official government equipment used in an official capacity.

l. PEDs shall be configured with appropriate security settings in accordance with reference (a) to reference (d). Blackberry devices will require specific security settings to include, but not limited to, the display of the standard DoD approved Warning Banner, Antivirus, and must meet current DoD minimum password requirements of eight alphanumeric characters. If capable, PED devices shall be set to require password re-authentication after a maximum of thirty minutes of inactivity.

m. PEDs owned by contracted companies may be authorized in the command in the performance of official contractor duties. The prohibitions for cameras and recording devices apply. No contractor owned PED will be connected to government NMCI or RDT&E systems without specific authorization by cognizant DAA.

5. Responsibilities

a. Command Chief Information Officer (CIO), Information Assurance Manager (IAM) and Security Officer shall:

(1) Ensure that PED use at the command is in accordance with this policy.

(2) Develop appropriate and effective processes for implementation.

(3) Ensure that all PEDs issued are properly configured prior to their issuance to users.

(4) Maintain this policy.

b. Program Managers of PED solutions shall:

(1) Implement this policy as applicable in their programs, to include careful consideration of the vulnerabilities and risks associated with the design of wireless solutions.

(2) Eliminate, upgrade or replace PEDs that do not comply with this policy.

6. Evolving Technologies and Policy. The marketplace for PEDs is very dynamic and rapidly evolving as wireless technologies continue to proliferate at rapid rates. It will be necessary to update and refine this policy as newer and more capable products become available. Additionally, any new policy from higher authority that prescribes more stringent restrictions than this policy document will be complied in. This PED policy is consistent with NMCI policy and will be reviewed on a regular basis to ensure that future versions of this policy are harmonized with NMCI products and policies.

7. Violations. Individuals violating the above policy are subject to confiscation of personal electronic equipment, possible forfeiture of government electronic equipment, appropriate administrative discipline, and notification to the Department of the Navy Central Adjudication Facility (DON CAF).

J. A. GREENE

Distribution:
https://cdsa.nmci.navy.mil/ Library Tab