



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3044 CATLIN AVENUE
QUANTICO, VIRGINIA 22134-5103

IN REPLY REFER TO:

5230

MRI

22 APR 2010

From: Chief Information Officer, Personal and Family Readiness
Division, HQMC, Quantico VA 22134-5099

Subj: INFORMATION TECHNOLOGY RESOURCES GUIDANCE

Ref: (a) DoD 5500.7-R, Joint Ethics Regulation 30 Aug 1993
(b) Marine Corps Enterprise Information Assurance Directive,
011 Personally Identifiable (PII), 9 April 2009
(c) MCO P1700.27B Marine Corps Community Services Policy
Manual

1. The Personal and Family Readiness Division (CMC MR) provides government owned communication systems that include, but are not limited to telephones, facsimile machines, personal computers, peripheral/portable devices, electronic mail (email), and internet systems. Per reference (a), the use of the equipment and systems shall be for official use and authorized purposes only. Reference (b) establishes Marine Corps policy on proper handling and protection of PII to prevent loss or compromise, and provides that all Marine Corps employees/contractors are responsible for safeguarding the privacy rights of others.

2. Personally Identifiable Information (PII). Reference (b) defines the definition of Personally Identifiable Information (PII) as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

a. Email. Email containing any amount of PII or attachments containing PII must be digitally signed and encrypted using DoD approved PKI certificates. The subject line of the email must begin with "FOUO". The body of the email shall contain a statement notifying the recipient to treat the email and its contents:

"FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE (FOUO). ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALITIES.

This statement will be applied to all email containing PII, even if it is encrypted.

b. Portable Electronic Devices (PEDs) and Removable Storage. Any PED (includes but is not limited to; Personal Digital Assistants (PDA), Blackberries, palm tops, hand-held/laptop computers, web enabled cell phones, two-way pagers, wireless Email devices, and audio/video recording devices) or removable storage device/media that processes or stores electronic records containing PII, shall be restricted to DoD owned, leased, or occupied workplaces, to include alternate workstations such as authorized telework sites.

c. Duty to Report PII Breach. MR employees and contractors shall immediately report all actual or suspected breach of PII to MRI, Chief Information Security Office, including loss of government computer-owned equipment containing PII. A breach of PII occurs when PII is lost, stolen, released without proper need, improperly distributed, or incorrectly disposed, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic where one or more individuals could be adversely affected. MRI will provide guidance and ensure compliance, as appropriate, with reference (b). Failure to report breaches of PII may result in civil or criminal actions against the employee, costly fines up to \$5000 per instance and jail time up to one year, in addition to adverse administrative personnel action.

3. Internet Access and Electronic Mail. Reference (c) provides guidance regarding internet access as well as electronic mail. Internet access is provided to staff members via the USMC-MCCS.org wide area network. Use of this network service affirms consent to monitoring, as with any other DoD interest computer system. Internet access and electronic mail usage are monitored daily for unauthorized access to sites considered to be repositories of sexual or pornographic materials, along with potential security violations. Email is monitored with a spam filter and anti-virus checker. The product also specifically searches for email with social security numbers or credit card numbers embedded in the email or in an attached document. All users should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy. Any misuse or evidence of violation of criminal statutes will be reported to the site administrator, Assistant Chief of staff or Director MCCS and/or law enforcement officials.

Any electronic material received, stored, or transmitted that is found to be offensive, detrimental, or of an inappropriate nature, content, or intent may be deleted from the system without notification.

a. Permissible Activities:

(1) Obtain information to support DOD/DON/Marine Corps missions.

(2) Obtain information that enhances the professional skills of Marine Corps personnel.

(3) Improve professional or personal skills as part of a formal academic education or military/civilian professional development program (approved by the Command).

(4) Personal internet searches and brief communications as long as it:

- does not adversely affect the performance of official duties by the Marine or employee.
- serves a legitimate public interest
- is of minimal frequency and duration and occurs during the individual's personal time
- does not overburden Marine Corps MCCS computing resources or communication systems

b. Prohibited use:

(1) Illegal, fraudulent or malicious activities; to include sending electronic mail that is harassing, insulting, or attacking in nature or electronic mail engaging in racial, gender or other slurs.

(2) Partisan political activity, political or religious lobbying or advocacy of activities on behalf of organizations having no affiliation with the Marine Corps of DOD.

(3) Activities whose purposes are for personal or commercial financial gain; e.g., online brokering, selling goods or services.

(4) Unauthorized fundraising

(5) Accessing, storing, processing, displaying or distributing offensive or obscene material, such as pornography and hate literature; harassing, insulting, or attacking others; engaging in racial, gender or other slurs.

(6) Obtaining, installing or using software obtained in violation of the appropriate vendors patent, copyright, trade secret or license agreement.

(7) Sharing of internet accounts.

(8) Access to or the providing of streaming media resources or other network services outside the purpose of conducting business. This includes, but is not limited to internet radio stations, streaming audio (MP3), unauthorized video streams, file transfer protocol (FTP), web and chat servers.

(9) Use of media/software sharing programs (e.g., Napster, Guntella, etc.).

(10) Creating or forwarding chain email.

(11) The use of 'taglines' in email signatures, whether for formal or informal purposes.

(12) The use of commercial email services for the storage or transfer of official email or data files.

4. Violations of security regulations or unauthorized use of information technology resources are subject to disciplinary action, up to and including termination.



L. J. CARUSO

Employee Signature

Date

Print Name