



UNITED STATES MARINE CORPS  
I MARINE EXPEDITIONARY FORCE  
U. S. MARINE CORPS FORCES, PACIFIC  
BOX 555300  
CAMP PENDLETON, CA 92055-5300

5200  
SSEC/G-6  
28 APR 2015

POLICY LETTER 6-15

From: Commanding General, I Marine Expeditionary Force  
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE (I MEF) POLICY FOR USAGE AND MANAGEMENT  
OF NETWORK STORAGE RESOURCES

Ref: (a) DoDM 5200.01-V3, DoD Information Security Program: Protection of  
Classified Information, February 2012  
(b) DON CIO WASHINGTON DC 031648Z Oct 11  
(c) USMC ECSD 011 Personally Identifiable Information (PII) V 3.0  
(d) IMEFO 5200.2, Governance Plan for I Marine Expeditionary Force (I  
MEF) Information Management/Knowledge Management (IM/KM) Portals,  
April 2015

Encl: (1) List of Unauthorized File Extensions/File Extensions  
Requiring Written Authorization from the Local Information  
Assurance Authority  
(2) File Exemption Request Form

1. Purpose. To ensure adequate storage capacity of I MEF shared drive  
resources on Marine Corps Enterprise Network Non-classified Internet Protocol  
Router Network (MCEN N) and the Marine Corps Enterprise Network Secret  
Internet Protocol Router Network (MCEN S) in accordance with reference (a).

2. Tasks

a. I MEF G-6 Systems Administrators

- (1) Establish internal enforcement procedures for this policy.
- (2) Ensure access control measures are complied with including  
technical, physical, personnel, and administrative control measures.
- (3) In accordance with reference (b), section (5), paragraph (d)  
ensure that organizational resources are utilized for official use only.
- (4) In accordance with reference (c), section (5.2) ensure files  
containing personally identifiable information (PII) are not stored on shared  
drive resources unless they are password protected and only accessible to  
individuals with an official need to know.
- (5) In accordance with enclosure (1) identify and remove all  
unauthorized file extensions.
- (6) Monitor shared drives for adherence to this policy.
- (7) Provide training in support of this policy.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is  
unlimited.

28 APR 2015

(8) Failure to comply with this policy will result in the deletion of data that is not policy compliant.

b. I MEF Information Systems Coordinators

- (1) Assign appropriate permission delegation to shared drive folders.
- (2) Replace individual or personally named folders with folders named for a billet or section.
- (3) Archive and remove aged files that have not been accessed within the previous 18 months.
- (4) Enclosure (2) may be utilized to request a waiver for official use data that is not compliant with this policy letter.

c. Information Owners

- (1) Ensure that data labeling of information aligns with its appropriate security classification.
- (2) In accordance with reference (d), section 7 ensure file naming and meta-data tagging conventions are followed.

3. Scope

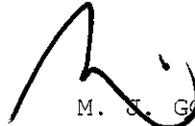
a. I MEF Command Element (CE), I Marine Expeditionary Force Headquarters Group (I MHG) units, Special Purpose Marine Air-Ground Task Force (SPMAGTF), and 11th, 13th, and 15th Marine Expeditionary Units (MEU) possess a limited amount of shared drive space allocated on assigned network storage locations. Current network storage resources lack quota management. Without the benefit of a share drive policy and quota management, the shared drives regularly fill up due to the storage of duplicate files, unauthorized files extensions listed in enclosure (1), and personal data causing disruptions to mission services.

b. This policy letter is applicable to I MEF CE, I MHG units, SPMAGTF, and 11th, 13th, and 15th MEUs.

4. Certification

a. Points of contact are the I MEF G-6 Helpdesk at DSN 365-9199, or commercial at 760-725-9199 or the I MEF G-6 Information Systems Management Office (ISMO) Chief at DSN 365-1545 or commercial at 760-725-1545.

b. This policy letter is effective the date signed.

  
M. J. GOUGH  
Chief of Staff

DISTRIBUTION: I/II

28 APR 2015

LIST OF UNAUTHORIZED FILE EXTENSIONS/FILE EXTENSIONS REQUIRING WRITTEN  
AUTHORIZATION FROM THE LOCAL INDIVIDUAL ASSURANCE AUTHORITY

1. Unauthorized File Extensions. The file extensions listed below are examples of unauthorized shared drive file types. The list is not intended to be a comprehensive list as multiple file extensions exist for similar file types and new file extension formats are created frequently.

a. **CLASSIFIED FILES OF ANY TYPE ARE NOT AUTHORIZED ON OR ALLOWED ON NIPRNET SHARED DRIVE SPACE. If Classified spillage is discovered take immediate Standard Operating Procedural steps pertaining to spillage.**

b. Any documents containing any variation of Personal Identifiable Information (PII) are not authorized to be on NIPRNET shared media storage space and must be immediately deleted if discovered.

c. Outlook PST files should not be stored on NIPRNET and SIPRNET shared space. PST files should be stored on the local C Drive or be backed up to an external device.

d. Multimedia files should not be stored on NIPRNET and SIPRNET shared drive space unless it is specifically identified as required (to support a presentation) and has been authorized by the local IA Authority. Multimedia files should be stored on external drives, CDRs or on local drives.

e. Any data that is executable (such as a back-up copy of software) should not be stored on NIPRNET and SIPRNET shared drive space. These files should be stored on external drives, CDRs or on local drives.

f. Aged files (files older than 18 months) should be archived to external drives, CDRs or DVRs.

g. Any unofficial data, such as personal pictures, jokes, etc., are not authorized in shared drive space.

2. Sample File Extension Types

.EXE - Executable File  
.PST - Outlook Personal Folder  
.OST - Outlook Offline Data File  
.3GP - Multimedia File  
.ACC - Graphics Account Data File  
.AIFF - Audio Interchange File Format  
.AU - Audio File  
.AVI - Audio Video Interleave File  
.BAT - Batch File  
.BIN - Binary File  
.COM - Binary Executable File  
.DCR - Raw Image or Media File  
.DLL - Dynamic Link Library File  
.FLV - Flash Video File  
.GIF - Graphics Interchange Format  
.JPG - Picture File  
.JPEG - Picture File  
.M4A - MPEG-4 Audio File  
.MIDI - Musical Instrument Digital Interface File

**2 8 APR 2015**

.MOV - QuickTime Movie File  
.MP3 - MPEG Layer III Audio File  
.MP4 - MPEG Layer 4 Visual/Audio File  
.MPEG - Audio/Video File  
.MPA - Audio/Video File  
.MPG - Audio/Video File  
.MPV - Audio/Video File  
.RM - RealMedia File  
.RAM - Real Audio Metadata File  
.RAR - Compressed Data Container File  
.SWF - ShockWave Flash File  
.THM - Video Thumbnail File  
.VBS - Visual Basic for Applications Script  
.VCF - Compressed Text File Format  
.VOB - DVD-Video Media File  
.WAV - Audio File Format  
.WMA - Windows Media Audio  
.WMV - Windows Media Video  
.ZIP - Compressed Data Container File

8 APR 2015

FILE EXEMPTION REQUEST FORM

File Requester/Data Owner Information

Name:		Phone:	
Unit:		Email:	
Section:			

ISC Information (N/A if same as above)

Name:		Phone:	
Unit:		Email:	
Section:			

File Information

File Name:	
Enclave (SIPR/NIPR)	
File Type (e.g.: Movie File):	
Requested File Location:	
File Owner (Section/Username):	

Reason for Exemption Request:


Requester Signature

ISC Signature

Unit/Section OIC Signature

ISMO Signature