USMEPCOM Acceptable Use Policy

(For use of this form see UMR 25-1)

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 9397 (Numbering System For Federal Accounts Relating To Individual Persons), DoDI 8500-01 (Cybersecurity), and AR 25-2 (Information Assurance).

PRINCIPAL PURPOSE: To ensure authorized individuals understand and agree with the usage and protection of information contained in USMEPCOM automation network(s).

ROUTINE USE(S): To be completed by each person annually that will be accessing the network. Filing will be maintained by the local Information Assurance Support Officer (IASO)

DISCLOSURE: Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to the USMEPCOM Network information systems.

REFERENCES: **DoDI 8500.01**, "Cybersecurity," March 13, 2014 Incorporating Change 1, Effective October 7, 2019
DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
DoDM 5 200.01 (Vol 4), "DOD Information Security Program: Controlled Unclassified Information (CUI),"February 24,2012
DoDD 5400.11, "DoD Privacy Program," October 29, 2014
DoDI 1035.01, "Telework Policy," April 4, 2012 Incorporating Change 1, Effective April 7, 2020
VVSP STIG "Voice Video Services Policy Security Technical Implementation Guide: Version 3, Release:17 October 25, 2019

1. Understanding.

I understand that I have the primary responsibility to safeguard the information contained within the USMEPCOM Networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use. I also understand that I will be held responsible for damage caused to a Government system or data through negligence or a willful act.

2. Access.

Access to this network is for official use and authorized purposes as set forth in DOD Regulation 5500.7-5 (Joint Ethics Regulation), AR25-2 (Information Assurance), and USMEPCOM policy and accreditation.

3. Revocation.

Access to USMEPCOM resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing.

NO Processing of classified information is authorized or allowed on the USMEPCOM network.

5. Unclassified information processing.

The IT Network is the primary unclassified system for USMEPCOM.

a. User must be a U.S. citizen to access USMEPCOM's Network.

b. The IT Network provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and Internet networking protocols such as Web Access and Virtual Private Network (VPN) and is approved to process UNCLASSIFIED Controlled Unclassified Information (CUI) and SENSITIVE CUI per DoDI 5200.01, volume 4 DoD Information Security Program: Controlled Unclassified Information (CUI). The USMEPCOM Approving Official (AO) has accredited this network for processing this type of information.

c. The NIPRNET and the Internet, for the purpose of the AUP, are synonymous. Email and attachments are vulnerable to interception as they traverse the NIPRNET (Non-secure Internet Protocol Routing Network) and Internet.

6. Minimum security rules and requirements.

As an IT Network user, the following minimum-security requirements apply:

a. Personnel are not permitted to access the Defense Accession Network (DAN) unless in complete compliance with the USMEPCOM personnel security requirements for operating in a Controlled Unclassified and sensitive environment.

b. I have completed DoD Cyber Awareness Challenge within annual requirements. I will participate in all training programs as required (including threat identification, physical security, acceptable use policies, malicious content and logic identification, and nonstandard threats such as social engineering) before receiving system access.

c. Government-furnished CACs will be the primary method of user authentication for access to government systems. If a username and password is required, I will generate and protect passwords and passphrases. Passwords will consist of 15 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not use as my user ID, common names, birthday, telephone numbers, military acronyms, call signs, or dictionary words as passwords or passphrases.

d. I will use only authorized government issued hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will not attempt to access or process data exceeding the authorized Information System (IS) classification level.

f. I will not alter or change the configuration or use operating systems or programs, except as specifically authorized.

g. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

h. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

i. I will not utilize USMEPCOM or DoD-provided ISs for commercial financial gain or illegal activities.
j. I will comply with all security guidance from USMEPCOM Information Assurance Personnel.
k. Maintenance will be performed by J-6 information technology specialists or MEPS ITSs only.
l. I will use screen locks, actively lock workstation, log off, and remove my Common Access Card from the workstation when departing the area of my PC. If I am going to vacate my workstation for an extended period to include at the end of the workday, I will log off completely.
m. I will immediately report any suspicious output, files, shortcuts, or system problems to the MEPS or sector ITS or USMEPCOM MIT Help Desk and cease all activities on the system.
n. Ensure that display or output of sensitive information in human-readable form is positioned to deter individuals from reading the information or obtain a privacy screen for your monitor.
o. Inform the supervisor when I no longer require access to a particular DoD information system or enclave.
p. Personal use of the information system is authorized ***if*** the following conditions are met:
   (1) Does not adversely affect the performance of official duties
   (2) Is made during employee's personal time
   (3) Does not reflect adversely on the Federal Government
   (4) Does not interfere with communications or network system functionality
   (5) Does not create any significant additional cost to DoD
q. Personal use of the information system is not authorized for the following:
   (1) To solicit, advertise, or engage in selling activities in support of a private business enterprise,
   (2) To promote fundraising activities
   (3) To send chain letters
   (4) To send harassing email
   (5) Downloading of video or voice files except when serving as an approved official USMEPCOM function.
   (6) Use of programs intended to scan networks and systems, such as port scanners and vulnerability scanners, or network sniffing tools used to collect user information and passwords unless authorized by the Risk Management and Compliance Office.
   (7) Use of user ID's of others is prohibited to include impersonation of another user.
   (8) Failure to follow existing security policies and procedures in the use of Internet services. Inclusive in this restriction is any action that might jeopardize the USMEPCOM Network and associated computer systems and data files (to include, but not limited to virus attacks when downloading files from the Internet).
   (9) Disclosure of Privacy Act material, copyrighted materials, and procurement of sensitive material without the appropriate clearances.
   (10) Use of the USMEPCOM Network while in violation of any USMEPCOM and Department of Defense Policies and Regulations, and the current license agreements.
   (11) Viewing, storage, or distribution of pornography or pornographic or obscene (adult or child) material.
   (12) Installation of unauthorized games on any USMEPCOM computer.

r. I understand that monitoring of the IT Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of USMEPCOM Information Systems: Storage of personal files obtained via the Internet may not be stored on Government PC hard drives or on local area network (LAN) servers.

Note: Personnel not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative, or prosecutorial actions.

7. Remote Access:

If I am granted remote access privileges, I understand:

a. Access will be routed through and approved by the user's supervisor. The supervisor will route to MEIT/J-6 for processing.
b. Remote access will be via virtual private network (VPN), or outlook web access (OWA). Government owned hardware and software will be used. The use of Virtual Private Network (VPN) software is mandatory to protect and control internal and external access to USMEPCOM information systems and networks. Immediate activation of the VPN session (after local logon) is required to ensure proper encryption to protect the confidentiality of the session and locally stored data.
c. USMEPCOM shall provide government furnished equipment, to include a computer with software, and communications capabilities with appropriate security measures as the primary means for remote access for any regular and recurring telework arrangement that involves CUI/Sensitive information.
d. Remote users must ensure that their computer is returned to the MEPS/HQ at least every 30 days. This will ensure the most current patches and updates for GFE are loaded. Supervisors of long-term teleworkers must ensure this requirement is met, in cases where the user is unable to return the equipment.
e. USMEPCOM IT administrators/privileged users must comply with the following requirements when accessing USMEPCOM networks from outside of the enclave:
   (1) After establishing a secure connection, elevate permissions to the appropriate level for conducting administrator tasks.
   (2) Terminate connection when administrator tasks are complete.
   (3) Safeguard information (i.e., do not access or display in an area where unauthorized persons are present) and control the equipment after connection termination.

8. Mobile Phones.

a. I will use the device in compliance with applicable state and local laws (i.e. while driving). This includes the use of various types of headsets designed to allow proper operation of issued device.
b. I will not operate a wireless device in areas where classified information is electronically stored or processed.
c. I will ensure the mobile handheld device is cradled or synced at least once every 30 days to receive updated keys and/or software updates.
d. I have completed wireless training at https://cyber.mil/training/dod-mobile-devices/
e. I am aware of the following risks when utilizing the SMS service:
   (1) Messages are not encrypted, and copies are stored in memory on the phone and in the wireless carrier database. Sensitive information should not be sent via SMS/Text/Messages/Multimedia Messaging Service (MMS).
   (2) I will not connect to an unauthorized URL.
   (3) Executable files (including malware) can be embedded in SMS/Text Message/MMS.
   (4) Photos sent via SMS/Text Messages/MMS can have URLs to hacker web sites or executable files (including malware) embedded in the photo or executable. When the photo is viewed or the executable is opened, the phone will connect to web site of the embedded web site.

9. Government Furnished Equipment Security.

Users of mobile computing devices (laptops, portable notebooks, tablet-PCs, and similar systems) are tasked with the physical security of these mobile devices. I will make every effort to ensure the physical security of any GFE assigned to me. Any failure to take proper precautions could result in revocation of Remote Access or Mobile Phone use. I understand that DoD Information Technology Equipment (ITE) issued to me to perform my official duties remains property of the Federal Government. I understand that I must return all ITE to the Federal Government (USMEPCOM) promptly when no longer needed to perform my official duties or when I am no longer an employee, contractor, or military member assigned, attached, or otherwise detailed to USMEPCOM. Failure to return government furnished equipment could result in criminal prosecution.

10. Voice-Video-over Internet Protocol (VVOIP) Security.

Voice-Video-over IP (VVoIP) endpoints include telephones, video-teleconferencing (VTC) systems, the Jabber soft client and the Microsoft Teams application (not managed by HQ MEPCOM).

a. Users of HQ MEPCOM VVoIP endpoints must protect the confidentiality of voice and video communications and adhere to the following:
   (1) Promptly report unauthorized or improper use of VVoIP end point voice, video or chat capabilities to the Information Assurance Manager, Security Manager and/or Physical Security Officer.
   (2) Comply with all security requirements when using the Cisco Jabber PC client and Microsoft Teams application.
   (3) HQ voice, video and chat connections are not secure
   (4) Employees must NOT share sensitive information over any VVoIP system or component.
   (5) This mandate also applies to disclosure via chat in applications such as Jabber, Microsoft Teams, Slack, and any other collaboration tools.
   (6) Onsite and Remote workers must comply with these requirements

b. MEPCOM VVoIP Endpoints are non-classified communications devices. Therefore, classified information should never be introduced or transmitted on them. Operation of Jabber, VTC codecs and all other VVoIP end points should always include physical and operational safeguards to protect sensitive information and ensure such information is not disclosed. All users are required to ensure operational safeguards by complying with the following:
   (1) Conference room and work/home users shall not place sensitive, potentially sensitive, CUI, or classified information on a table, desk or wall within the view of the camera(s) without proper protection (e.g., a proper cover)or at such an angle that the camera(s) could focus on it.
   (2) Conference room and work/home office users shall not read or view sensitive or classified information
   (3) Users must move, cover, or power off monitors and displays capable of showing such information
   (4) Users shall disable computer built-in or accessory cameras when they are not in use.
   (5) Users must take care to share only what is required.

c. VVoIP users must safeguard potentially sensitive, CUI, or classified speech by complying with the following:
   (1) Users must mute their microphones, including those on headsets, when not actively participating in discussion, such as when not speaking, before and after conference sessions, and during conference breaks.
   (2) Users shall not position their microphones or headsets where non-participant conversation can be captured and transmitted.
   (3) Users must keep the volume settings of speakers and headsets low enough to prevent non-participants from hearing call or conference information.

d. Only MEPCOM purchased and owned VVoIP equipment may be connected to the MEPCOM network. Bluetooth, DECT/DECT 6.0, and other RF wireless accessories are not authorized for use. Personal VVoIP technology is not authorized to for use on the MEPCOM network. Personal VVoIP technology includes non-government provided hardware (IP phones) and software phones to include Skype, etc. Any use of personal VoIP technology will be reported to the MEPCOM Cyber Security Office (CSO) for action.

e. Users must not install any application or agent, to include UC soft clients, VTC software, or IM client that connects to or uses a public VoIP or IM service for non-official business or communicates peer-to-peer with other applications, agents, or personal phone gateways.

f. No bridging equipment of any type will be connected to the VVOIP equipment.

g. Only government-approved Instant Messaging (IM) or Unified Capabilities (UC) soft clients will be used on Government Furnished Equipment (GFE).

11. USMEPCOM Wireless Operations at HQ and the MEPS.

a. The IT network is comprised of wired and wireless networks. Only Government furnished equipment is permitted to connect to the government furnished networks.
b. Wireless network IDs and passphrases are not permitted to be shared to non-USMEPCOM personnel.
c. Wireless networks are limited in bandwidth, and I agree to use sparingly, only when necessary.
d. When using USMEPCOM wireless network, I will treat it as a wired network with all applicable rules and regulations.

Acknowledgment: I have read the above regulations. I understand that the information below will be used to identify me and may be disclosed to law enforcement authorities for investigation or prosecuting violations. I understand my responsibilities regarding these systems and the information contained in them. In order to maintain access to USMEPCOM computing systems, all users must review and agree to the USMEPCOM Acceptable Use Policy (AUP).

_____