Acceptable Use Policy

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the Installation Management Command Application Service Provider (IMCOM ASP) and the Installation Management Command Commercial Application Service Provider (IMCOM CASP) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

2. **Access.** Access to the IMCOM ASP and IMCOM CASP is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Classified information Processing**. The IMCOM ASP and IMCOM CASP is an FOUO Information System (IS) for IMCOM and MWR community. The IMCOM ASP and IMCOM CASP is a CONUS and OCNUS system approved to process only up to FOUO information.

    a. T h e IMCOM ASP and IMCOM CASP is authorized for FOUO processing in accordance with accreditation package number, identification, etc.

    b. T h e IMCOM ASP and IMCOM CASP are also US-only systems and not accredited for transmission of NATO material.

    c. The ultimate responsibility for ensuring the protection of information lies with the user. The release of classified information through the IMCOM ASP and IMCOM CASP is a security violation and will be investigated and handled as a security violation or as a criminal offense.

5. **FOUO information processing**. IMCOM ASP and IMCOM CASP are authorized to process FOUO information.

6. **Minimum security rules and requirements.** As a IMCOM ASP and IMCOM CASP system user, the following minimum security rules and requirements apply:

    a. P e r s o n n e l are not permitted access to the IMCOM ASP and IMCOM CASP unless in complete compliance with the IMCOM personnel security requirement for operating in a FOUO environment and have a business need-to-know.

    b. I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 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 my user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)

d. I will not attempt to access or process data exceeding the authorized FMWRC MIS ASP
classification level.

d. 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.

f. 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.

g. I will not utilize the IMCOM ASP and IMCOM CASP for commercial financial gain or illegal activities.

h. Maintenance on the IMCOM ASP and IMCOM CASP will only be performed by an authorized System Administrator (SA).

i. I will log off the IMCOM ASP and IMCOM CASP portal when departing the area.

j. I will immediately report any suspicious output, files, shortcuts, or system problems to the IMCOM ASP and IMCOM CASP SA and/or IASO and cease all activities on the system.

k. I will address any questions regarding policy, responsibilities, and duties to the IMCOM ASP and IMCOM CASP SA and/or IASO.

l. I understand that the IMCOM ASP and IMCOM CASP platform is the property of the Army and is provided to me for official and authorized uses. I further understand that each IMCOM ASP and IMCOM CASP is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IMCOM ASP and IMCOM CASP and may have only a limited expectation of privacy in personal data on the IMCOM ASP and IMCOM CASP. I realize that I should not store data on the IMCOM ASP and IMCOM CASP that I do not want others to see.

m. I understand that monitoring of the IMCOM ASP and IMCOM CASP 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 IMCOM ASP and IMCOM CASP:

- Unethical Use (e.g. spam, profanity, sexual misconduct, gaming, extortion)
- Accessing and showing unauthorized sites (e.g. pornography, streaming videos. E- bay, chat rooms)
- Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use

(e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).

- To show what is deemed unethical (e.g., spam, profanity, sexual content, gaining).

- To show unauthorized services (e.g., peer-to-peer, distributed computing).
  (Note: Activity in any criteria can lead to criminal offenses.)

7. **Standard Mandatory Notice and Consent Provision for All DoD Information System User Agreements**
   By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

   a. You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

   b. You consent to the following conditions:

      (1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

      (2) At any time, the U.S. Government may inspect and seize data stored on this information system.

      (3) Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

      (4) This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

      (5) Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
         (a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counter intelligence investigation against any party and does not negate

any applicable privilege or confidentiality that otherwise applies.

(b) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

(c) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

(d) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

(e) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

(6) In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counter intelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

(7) All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless o whether the banner expressly references this User Agreement.

8. **Acknowledgement.** The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to (insert your organization) information systems. I have read the above requirements regarding use of (insert your organization) access systems. I understand my responsibilities regarding these systems and the information contained in them.

Directorate/Division/Branch	Date
Last Name, First, MI (print)	Rank/Grade
Signature	Area Code and Phone Number
Supervisor: Last Name, First, MI (print)	Date
Signature	Area Code and Phone Number