DEPARTMENT OF THE AIR FORCE MOBILE DEVICE USER AGREEMENT

The policy described in this memorandum is in accordance with Air Force Instruction AFI 10-701, *Operations Security (OPSEC);* Department of the Air Force Manual (DAFMAN) 17-1301, *Computer Security (COMPUSEC)*; DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*; Department of Defense Instruction (DoDI) 5000.64_DAFI 23-111*, Accountability and Management of DoD Equipment and Other Accountable Property;* AFI 17-130, *Cybersecurity Program Management;* DoDI 8500.01*, Cybersecurity;* Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); and DISA Security Requirements Guides (SRGs).

AUTHORITY: DoDI 8500.01, AFI 10-701, DAFMAN 17-1301, DAFMAN 17-1203, DoDI 5000.64_DAFI 23-111, and AFI 17-130.

PRINCIPAL PURPOSE: To ensure users are made aware of, and consent to, Department of Defense (DoD) and Department of the Air Force (DAF) monitoring policies and procedures.

ROUTINE USES: May be disclosed for the purpose of verifying individuals were made aware of monitoring policies and procedures. The DoD's Blanket Routine uses for law enforcement and similar purposes apply.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of this request. This form requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized Department of Defense Instruction (DoDI) 5400.11, *DoD Privacy and Civil Liberties Programs*. The applicable System of Record Notice (SORN) F017 SAF CN A, *Bring Your Own Approved Device (BYOAD),* is available at: **https://dpcld.defense.gov/Privacy/SORNs/**.

PRESCRIBED BY: Department of the Air Force Manual 17-1301.

AUTHORIZED USE/ACCESS TYPE: End-user exclusively.

PART I - PERSONAL INFORMATION

(To be completed by end-user)

1. LAST NAME	2. FIRST NAME	3. RANK/GRADE
4. ORGANIZATION	**5. TELEPHONE NUMBER**	**6. WORK E-MAIL ADDRESS**

7. PURPOSE: Select all that apply

- ☐ **U.S. government-issued Mobile Device(s)**. *Please complete Part II, and adhere to Parts III-IV, and sign below.*
- ☐ **DAF Approved Mobile Device (AMD) formerly BYOAD program**. *Please adhere to Part V, and sign below.*
- ☐ **AMD Virtual Mobile Infrastructure (VMI).** *Please adhere to Part VI, and sign below.*

PART II – PORTABLE ELECTRONIC DEVICE INFORMATION

If multiple mobile devices are assigned to an individual, document all devices in Block 12 or on another locally created sheet and affix to this user agreement. Only one user agreement is required to be signed, given all devices are appropriately documented. If a mobile device is shared by multiple users, each user must complete this user agreement and list all applicable devices.

8. DEVICE TYPE	9. DEVICE MODEL	10. DEVICE TELEPHONE NUMBER	11. SERIAL NUMBER

12. ORGANIZATION DEFINED REQUIREMENTS *(e.g., Common Access Card (CAC) Sled Serial #, International Mobile Equipment Identity (IMEI)/International Mobile Equipment Identifier (MEID), SIPRNet Token, and Subscriber Identification Module (SIM), etc.)*

13. REMARKS AS NEEDED

By signing this Agreement, I confirm acceptance of the relevant Parts based on the selected "Purpose" in "Part I" and agree to abide with their terms and conditions.

14. DATE SIGNED (YYYYMMDD)	15. SIGNATURE OF USER

NOTE: This signed Mobile Device User Agreement will be retained by the CSS or the designated representative for a minimum of six months after the device has been returned to the issuing office.

PART III - SECURITY REQUIREMENTS

The following preventive measures are required to ensure that the use of mobile devices does not result in the release of DoD information to unauthorized persons.

1. I understand that this mobile device is provided for the official U.S. Government and is authorized for exclusive use. Only authorized information may be stored on or transmitted by this device. Misuse of this device (use outside of official U.S. Government and authorized purposes) may subject me to appropriate administrative, disciplinary, criminal, or other adverse actions.
2. I am the only individual authorized to use the mobile device. If a shared mobile device is assigned to me, I will ensure I document the times in which I have possession of the device I am responsible for physical damage to the device and the confidentiality and integrity of data on the device. Any damage caused will be immediately reported to my Commander's Support Staff (CSS).
3. I understand that if this device is lost or stolen, I must immediately report it to the Service Desk, my CSS, and if it is a classified mobile device, my security manager.
4. I understand the mobile device must be technologically (logical access) and physically secured. I will maintain device accountability at all times.
5. I agree that I will follow all security measures and requirements. I will complete annual mobile training requirements identified in DoD/Air Force policy, applicable DISA STIGs, and SRGs.
6. I understand that if I notice unusual activity, malfunctions, or abnormalities of this device, I will immediately report and return the device to the Service Desk or my CSS. I will not use or attempt to fix the device as it may have been compromised.
7. I will not connect this device to other computing equipment, including personal laptops (e.g., tethering or wireless personal area network [WPAN], air card use, and device synchronization [hot-synch]) without prior Authorizing Official (AO)/Designated Accrediting Authority (DAA) approval. I will also observe device-specific stipulations prior to any connections. I will not exceed my authorized user access and enable unauthorized functionality of this device. I will follow any local Mobile Remote Access connection policies and approval procedures prior to use.
   a. I acknowledge that I am allowed to connect to hotspots, personal Wi-Fi, and public Wi-Fi if I use an approved connection solution (i.e., Virtual Private Network (VPN)) and it is employed immediately after connection. Compliance with remote work and/or telework requirements must be adhered to in order for this to be applicable. Connections to DoD devices or networks require the device to be identified within an RMF package.
   b. I acknowledge that if this device has cellular capability that, I am only allowed to use cellular capability in an approved manner. If approved as part of an RMF package, I must use it as required. If it is not approved as part of an RMF package, it is NOT allowed to process, store, or transmit sensitive data (i.e., CUI, PII, etc.). Additional information and clarification can be obtained from the Communication Squadron, Information System Security Manager (ISSM), etc.
   c. I acknowledge that I am NOT allowed to make a direct or remote connection with any other device, regardless of type unless it is in line with paragraph 7.a or paragraph 7.b.
8. If issued a Smartphone device and Wi-Fi access is authorized, I will follow local command connection policies and conditions governing when and where the smartphone device may be connected to Wi-Fi access not controlled by DoD.
9. I understand that mobile devices connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation or connected via RJ-45) are not permitted simultaneous wireless operation. I will not configure the device to function as ad an hoc wireless access point to connect other mobile devices to the DoD-wired network.
10. I understand mobile devices are not approved for handling/storing sensitive/classified information unless properly encrypted and authorized.
11. I understand that I must exercise discretion (operations security) at all times when using government-issued mobile devices. During use, I will position this mobile device display to prevent the inadvertent disclosure of viewed information by unauthorized users.
12. I understand when transferring sensitive DoD information with this mobile device, I must sign and encrypt messages using DoD Public Key Infrastructure (PKI) credentials.
13. I acknowledge that unclassified mobile devices with digital cameras (still and video) are not allowed in any area where classified documents or information are transmitted, received, stored, or processed without AO approval.
14. I understand that this mobile device is not secure and will not be used to transmit, receive, store, or process classified information.
15. I understand that if classified information is inadvertently sent, accessed, or stored on this device, I must immediately turn off and/or remove the battery from the device and contact the Service Desk and my CSS to report as a data spill incident.
16. I acknowledge I will not use this mobile device within 3 meters (9.8ft) of any classified environment/data equipment unless authorized by the AO. I understand additional local and/or program restrictions may be required.
17. I will not configure mobile devices to download, install, or use unauthorized applications, software updates, or personal e-mail accounts (e.g., AOL, Yahoo, Gmail, etc.) unless authorized by the AO.
18. I acknowledge that only authorized wireless peripherals and Bluetooth devices (including CAC readers, headsets/hands-free devices) will be used/synchronized to this mobile device, and I must contact the Service Desk and/or my CSS for a list of approved devices.
19. I acknowledge that messaging applications (Short Message Service (SMS) and Multimedia Messaging Service (MMS), or similar capabilities) are provided only to individuals who have been granted approval by the AO or his/her assigned representative. Information exchanged between unclassified mobile devices using messaging applications is not authorized for the transmission, receipt, storing, or processing of Controlled Unclassified Information (CUI, e.g., FOUO information), Privacy Act (PA) information, Personally Identifiable Information (PII).

20. I understand locally or program-created operating instructions on the use of mobile devices may accompany this user agreement.

21. I acknowledge receipt of and responsibility for IAW AFI 17-130 and DoDI 5000.64_DAFI 23-111 for the items described and will return the device when no longer needed.

FOR REPORTING PROBLEMS, INCIDENT HANDLING, OR TO ASK QUESTIONS, CONTACT THE CSS OR SERVICE DESK

PART IV- ACKNOWLEDGMENT AND CONSENT

(Per DoD CIO Policy, the following acknowledgment and consent statement shall be included in all DoD information system user agreements.)

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

1. 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.

2. You consent to the following conditions:

   a. 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, network operations, and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

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

   c. 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 authorized purposes.

   d. 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.

   e. 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 products are private and confidential, as further explained below:

      (1) 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 network 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.

      (2) 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 counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

      (3) 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 protection of a privilege or confidentiality.

      (4) 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.

      (5) 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.

      (6) 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.

   f. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., 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.

   g. 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 of whether the banner expressly references this User Agreement.

PART V- APPROVED MOBILE DEVICE (AMD) USER AGREEMENT

Please review this section only if you select "DAF AMD" (question#7) as the intended purpose for signing this user agreement.

The DAF Approved Mobile Device (AMD) program allows military members and civilian employees to use their approved personal devices (i.e., smartphone or tablet) to access unclassified government information and applications by installing a Managed Mobile Service (MMS) on their personal devices. This program is completely voluntary and is for the convenience of the employee. Your acknowledgment of responsibilities and agreement below is required for the installation of a government-furnished MMS on your personal device. You access to DAF systems can be revoked if you agree to participate in this program and you subsequently violate terms of this agreement. Further, violating this agreement could subject you to disciplinary action in accordance with the Uniform Code of Military Justice (UCMJ), or the Civilian Personnel procedures as outlined in DAFI 36-148, Discipline and Adverse Actions of Civilian Employees, or other applicable Federal law.

1. You may only use an approved National Information Assurance Partnership (NIAP) device or a device that is both part of a pre-existing NIAP-compliant device family and undergoing NIAP evaluation for trusted devices to participate in the AMD program. This ensures separation and protection of DoD information. Devices that fail to achieve trusted device NIAP-compliant status are not eligible for AMD program use. You can find a list of NIAP-compliant products and a list of products under NIAP evaluation at **https://www.niap-ccevs.org**.
2. You must ensure that the latest applicable operating system (OS) and security patches are installed on your device(s); you have 30 days to be in compliance after public release of the most recent update. Failure to comply may result in loss of access to AMD provisions/capabilities.
3. You must have a device-unlock passcode, Personal Identification Number (PIN), or biometric enabled on your device.
4. You agree to allow the government to install application(s), other appropriate control mechanisms (i.e., the MMS), or both on your personal device. These provisions enable the government to maintain secure access control over official government applications, information, and services. The MMS and other applications are considered government-furnished equipment, and you agree to take reasonable precautions to secure your device.
5. You are responsible for all costs (e.g., data usage, roaming charges, device, equipment installments) associated with your commercial wireless provider agreement(s).
6. You will only access non-public Department of Defense (DoD) systems and DoD information through MMS.
7. You agree not to store any DoD non-public information outside of the MMS. However, you may access/download/store your Privacy Act protected data on your personal device outside of the MMS.
8. You freely and voluntarily consent to government monitoring and collecting information from the MMS on your personal device when using the U.S. Government Information Systems MMS feature.

   a. The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

   b. At any time, the USG may inspect and seize data stored on this IS.

   c. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

   d. This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.

   e. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential.
9. You agree that you are the primary user of the device, and you will not allow anyone else, including family members, to access the MMS or use the device while the MMS is open.
10. You adhere to appropriate Operational Security (OPSEC), including the possible removal or restricted use of the MMS, when traveling outside of the United States.
11. By participating in this program, you consent to surrender your personal device to the appropriate authorities if you are suspected of a security incident. As such, your personal phone may be held for investigative or law enforcement purposes, and the MMS is subject to search. It is always encouraged that you backup all personal data on your device.
12. You agree to report seized, lost, or stolen devices or any security incidents (e.g., malware, viruses, or unexplained software installs) to your security manager and the MMS helpdesk within 60 minutes.
13. All civilian personnel will comply with the applicable time and accounting policies. Work schedules and hours of duty may be modified as necessary, but are subject to local management procedures and approval, as well as collective bargaining agreement requirements.
14. Users who actively try to subvert security controls (e.g., bypassing rooting/jailbreak detection) may be subject to disciplinary action in accordance with the Uniform Code of Military Justice (UCMJ), the Civilian Personnel procedures as outlined in DAFI 36-148, or other applicable Federal law.
15. The government will make all reasonable attempts to maintain secure and usable AMD products and services; however, they are provided on an "as is" and "as available" basis. The government makes no representations or warranties of any kind, express or implied, as to the operation or the information, content, or materials included on or otherwise made available to you through the AMD program. You expressly agree that your use of these products and services is at your own risk. To the full extent permissible by applicable Federal law, the government disclaims all warranties, express or implied, including but not limited to implied warranties of merchantability and fitness of these services and products.
16. The DAF attempts to remove and mitigate all threats, but the government does not warrant that the MMS, information, content, or materials included on, or otherwise made available to you through the MMS are free of viruses or other harmful components. The government will not be liable for damages of any kind arising from the use of the MMS from any information, content, or materials included on or otherwise made available to you through the MMS, including but not limited to direct, indirect, incidental, punitive, and consequential damages.

By signing below, you acknowledge your rights and responsibilities and agree to participate in the AMD program. This acknowledgment is required for your access and use of official non-public government data on your personally-owned device.

PART VI- AMD VIRTUAL MOBILE INFRASTRUCTURE (VMI) USER AGREEMENT

Please review this section only if you select "DAF AMD VMI" (question#7) as the intended purpose for signing this user agreement.

The following preventative measures are requirements to ensure that the usage of the Authorized Mobile Device (AMD) Virtual Mobile Infrastructure (VMI) solution on a government furnished, non-government furnished device, or both with the goal of allowing access into the DoD information network does not result in the release of Department of Defense (DoD) information to unauthorized persons.

The AMD VMI solution aims to allow leaders, airmen/guardians, federal civilian employees ("user"), and contract personnel to use their personal electronic communication or mobility devices, i.e., smartphone or tablet, ("devices") to access unclassified government information and applications by installing a VMI application on their personal devices.

The AMD VMI program is completely voluntary and is for the participant's official use. Use of a personal device to conduct government business is not a right, condition, or duty of employment. By participation in this program users consent to terms outlined in the "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement" as required when accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only. Therefore, the user's acknowledgement of responsibilities and agreement below is required to install government- furnished AMD VMI application on a personal device. Access to Department of Defense (DoD) systems can be revoked and the user could be subject to disciplinary action in accordance with the Uniform Code of Military Justice (UCMJ) or civilian disciplinary procedures where a user agrees to participate in this program and subsequently intentionally or unintentionally violates any term in this agreement.

By participating in the AMD VMI capability deployment and signing this document, the user consents to and acknowledge that:

1. Only approved mobile device hardware manufactures running officially supported Apple iOS and Android operating systems (OS) software versions are authorized to participate in the AMD VMI program. Windows 10 and Windows 11 devices running latest DAF-approved patches for their respective operating systems (OS) software versions are authorized to participate in the AMD VMI program. The regularly updated list of approved mobile hardware devices, their associated operating systems, and Windows patch levels can be found in **https://armyeitaas.sharepoint-mil.us/sites/hypori/SitePages/User-Guides.aspx** under the title "VMI Device and Operating System." Outdated or unsupported operating systems will not be allowed to access AMD VMI application until updated to a supported version.
2. Management reserves the right to revoke an individual's access to the AMD VMI Application and subsequently suspend rights for access into the DoDIN.
3. The U.S. Government routinely intercepts and monitors communications within government information systems for purposes including, but not limited to, penetration testing, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations. Any communications initiated through the AMD VMI solution is subject to disclosure or usage for any U.S. Government-authorized purpose.
4. At any time, the U.S. Government may inspect and seize data stored within the AMD VMI application. THIS DOES NOT include seizing a personal device or personal data on the device.
5. This information system includes security measures (for example, authentication and access controls) to protect U.S. Government interests - not for the user's personal benefit or privacy.
6. Use of the AMD VMI:

   a. Users acknowledge that they may incur additional provider charges, fees, or both when the AMD VMI solution is used outside of the approved geographic area where the service was registered.

   b. Users may have their access restricted based on in place security and access controls without prior coordination and approval.

7. Users will be responsible for any improper usage of this application while enrolled.

   a. Users must immediately report any application issues/malfunctions to the designated capability managers for issue identification and resolution.

   b. Users shall immediately report any lost device(s), including user-registered devices containing the AMD VMI application, to the Army Enterprise Service Desk (AESD) or respective organizational AMD official for device accountability and reporting.

   c. User access to this program may be accepted and revoked at command discretion, based on command requirements/priorities.

   d. Use must notify AESD to de-provision their account in AMD when the user's requirement for the AMD VMI capability ends.

   e. User must abide by the state and local laws governing the use of mobile cell phones and smartphones while driving.

   f. User may be required to surrender data associated with AMD VMI application profile. As a result, user may lose all access rights to VMI profile in the event an inspection or forensic assessment is required for law enforcement or information security. This data pertains solely to the virtual environment and does not include personal data.

8. The Point of Contact (POC) and communication team for this capability deployment will be outlined in the Special Instructions section. Users may reach out to local capability managers, as necessary.

9. The user acknowledges that screenshots are not permitted inside the AMD VMI environment. Users are prohibited from recording images or sounds from an external device when using the AMD VMI application. Attempts at doing so result in capability suspension and AMD virtual data seizure and review.

10. Authentication and user access for the HQDA AMD pilot capability will be done by utilizing EAMS-A Mobile Connect and Purebred or other approved and authorized tokens/solutions.

11. User agrees to allow the government to install application(s) and other appropriate control mechanisms on user's AMD VMI application (virtual environment) to remain compliant with relevant security policies and directives. These provisions enable the government to maintain secure access control over official government applications, information, and services.

12. User agrees that they are the primary user of the device, and will not allow anyone else, including family members to access the AMD VMI application or to use the device while the AMD VMI application is open/running.

13. User will adhere to Operational Security (OPSEC), which may include the removal or restricted use of the AMD VMI application, depending on current policies and directives.

14. User freely and voluntarily consent to applicable site conditions and government monitoring and collection when accessing secured U.S. Government Information Systems through the AMD VMI feature,

15. All civilian personnel will comply with the applicable time and accounting policies. Work schedules and hours of duty may be modified as necessary but are subject to local management procedures and approval and collective bargaining agreement requirements.