DoD Mobility Unclassified Capability (DMUC) End User License Agreement

Last Name: **First Name:** **Organization:** MEARNG

Commercial / DSN Phone Number: 207- **NIPR Email Address:**

Device: iPhone 13 **Serial Number:**

DEVICE AND NETWORK SECURITY

- You are NOT authorized to connect a DMUC mobile device to any government or personal computer or laptop.
- Unapproved connections of the device will result in non-compliance and service suspension.
- DISA Personnel Only: You must download, install, and use the Cisco AnyConnect virtual private network (VPN) app from the DoD Mobile Application Store (MAS). The Cisco AnyConnect VPN must always be enabled and used for all network connections.
- You must adhere to the password complexity policy when you provision the device and this feature must remain enabled. All Apple iOS passcodes and Samsung device passwords must have a minimum of six (6), non-sequential, alpha-numeric characters. Samsung Galaxy KNOX passwords have a minimum of six (6) alpha-numeric characters, which is the minimum allowed by MobileIron. Disabling or not enabling this feature during the provisioning process will flag your device as non-compliant and your device will be wiped.
- Your device will be removed from the DMUC network if you make any changes to it that would prohibit the DMUC Mobile Device Manager (MDM) from managing it such as removing the DISA MDM profile (iOS) or disabling Device Administrator (Android). You may remove the DISA MDM profile and immediately reenroll an iOS devices to resolve an email connection error.
- If you suspect your device has been compromised, immediately open a trouble ticket with the help desk at your local command and contact your security manager. A compromising event may include, but is not limited to: unauthorized password change, function or feature change, mobile apps unexpectedly appearing on the device, etc. The device will be wiped of its data, applications (apps), and the service suspended.
- Commercial Wi-Fi networking is allowed only on trusted Wi-Fi networks with WPA2-Personal security. A trusted commercial Wi-Fi network, per IAW CMD Policy V2R3 STIG, WIR-SPP-010, is defined as a site-managed Wi-Fi access point connected to the internet only (Internet Gateway Only Connection) or a home Wi-Fi network (user managed). Public or hotel hotspots are NOT allowed.
- When using a DMUC mobile device's hotspot, WPA2 encryption must be enabled and you must change the device name to something that is not meaningful (e.g., site name, product name, room number, end user's name) and change the manufacturer's default hotspot password before use. The hotspot must be turned off when not in use. Please reference the iOS and Android Hotspot Quick Reference Guides for further instructions and appropriate implementation of Wi-Fi tethering.
- Devices MUST be used in accordance with DoD/local security and wireless policies.
- You MUST not engage in any activity that interferes with the DoD network or any services available on the DoD network.
- Removable media (e.g., SD card, micro-SD card) MUST NOT be used with your DMUC device.
- Personally Identifiable Information (PII) or any FOUO documents MUST not be transmitted to a non-Government controlled entity.
- Only update your mobile device operating system (Android, iOS) when notified by DISA.
- After 30 consecutive days of non-usage, your account is marked as inactive and may be deleted from the MDM.
- Classified material is NOT authorized on the device, contact your security manager for all security violations.
- Device MUST be turned off during any classified discussions.
- Device MUST NOT be used within three meters (nine feet) of a Secret Internet Protocol Router (SIPR) workstation.

DEVICE FUNCTIONALITIES / CAPABILITIES

- Bluetooth is permitted but must be in accordance with the "DMUC Authorized Device Memorandum," located on the Mobility User Corner, or DoD STIG approved Bluetooth devices. No other Bluetooth devices are permitted to pair or connect to DMUC devices. Bluetooth devices must stay within 3 feet of the mobile device while it is enabled and operational. When the device is not in use, the Bluetooth option must be disabled.
- Global Positioning System (GPS) is available for use on your device and can ONLY be used with approved applications and must be turned off when not in use. NOTE - GPS is a tracking device while it is active; therefore, you must check with your OPSEC office for guidance on using this feature, prior to travelling outside the United States.
- The following features on Apple devices are NOT approved for use and must not be enabled: Sharing location data via iCloud, iCloud Find my Phone, iCloud backups, storing PII in the Health App, Apple Pay, sending Diagnostic data, Near Field Communications (NFC), associating payment information with Apple ID and using a personal Apple ID.
- The following features on Samsung devices are NOT approved for use and MUST NOTE be enabled: S Voice, USB Storage, Export KNOX Calendar/Contacts to Personal mode, nearby devices, screen mirroring, manual date time change, Wi-Fi direct, physical/USB Wi-Fi Tethering, Bluetooth File Transfer, Message Preview on lock screen, Multi-user mode (tablets only), Smart Lock, Android Device Manager, and Development Mode .
- You must not set up or enable a Google account, Samsung account, Find my Mobile, sending Google Crash Reports, sending Diagnostic or Usage Data, and carrier backups or cloud-based capabilities, on Samsung devices. The DMUC Device Set up/Registration User Guide provides instructions on skipping these steps.
- Fingerprint authentication is authorized for the KNOX container, but NOT for accessing the Samsung Android device.
- You are not authorized to add 3rd party (Non-DEE or NGA) email accounts nor sync contacts or calendar events between public applications to the device (e.g., Google Gmail, Hotmail, Yahoo mail).
- You are not authorized to move your Defense Enterprise Email (DEE) calendar information outside of the Knox container on your Android device.
- You are not authorized to enter developer mode on your device.
- You are not authorized to print from your device.
- DoD Mobility PMO maintains a list of authorized applications in the Mobile Application Store (MAS) for your device (Mobile@Work for Android, and P.U.M.A. & DoD Apps for iOS devices). Downloading unapproved or third party applications will result in your device being flagged for non-compliance and potentially removed from the DMUC MDM.

ACCOUNTABILITY OF GOVERNMENT MOBILE DEVICES

- If your device is lost or stolen, you are required to immediately, open a trouble ticket with the help desk at your command with the user's name, device type to include; phone, serial and IMEI number, so the device can be removed from the MDM, and its service suspended.
- Users are responsible for the safekeeping and accountability of their device. Failure to do so may result in a Report of Survey or a statement of charges per your organizations policy.
- You will not use the device in any manner that would constitute a criminal offense or give rise to civil liabilities.
- You are prohibited from: accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity or violates any applicable local, state, federal, national, or international law.

By signing my name below, I affirm that I have read the above and understand the DoD funded mobile device services are For Official Use Only. I will abide by the rules governing proper use and security of the mobile device assigned to me.

I have completed all provisioning steps and agree to have my device removed from any previous MDM.

I acknowledge that I have read, understand, and agree to comply with the restrictions and requirements set forth in this agreement and ANNEX.

Signature: **Date:**

DEFENSE INFORMATION SYSTEMS AGENCY
DoD Mobility Program Management Office

ANNEX

U.S. GOVERNMENT INFORMATION SYSTEMS

DoD CIO Memorandum, “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement,” May 9, 2008 Requirements Incorporating Change 5, September 25, 2013:

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

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.

You consent to the following conditions:

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