ARMY IN EUROPE MOBILE DEVICE USER AGREEMENT

(AE Suppl 1 to AR 25-13)

Part I — Personal Information

This information may be used to contact a mobile-device user in the event of an emergency, security incident, or other requirements relating to the user's mobile device.

1. **Name** (First MI. Last)	2. **Grade or civilian status** (GS, LN, SES)	3. **Organization or unit**
4. Kaserne or installation	**5. Building**	**6. Room number**
7. Work telephone number	**8. E-mail address**	

Part II — Mobile Device User Agreement

The following policy and procedures are to ensure appropriate and economical use of mobile devices:

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 DOD information systems (ISs) you—

- Understand that the following policy and procedures apply equally to any device attached to that United States Government (USG) IS.
- Are accessing a USG IS that is provided only for USG-authorized use.
- Consent to the following conditions for use:
  - ○ This IS includes security measures (for example, authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
  - ○ Communications using and data stored on this IS are not private; are subject to routine monitoring, interception, and search; and may be disclosed or used by USG agencies for any USG-authorized purpose.
  - ○ At any time, the USG may inspect and seize data stored on this IS.
  - ○ The USG routinely intercepts and monitors communications transmitted by this IS for purposes that include, but are not limited to, penetration testing; communications security (COMSEC) monitoring; network operations and defense; and personal misconduct, law enforcement (LE), and counterintelligence (CI) investigations.
  - ○ Using an IS does not constitute user consent to searching or monitoring for personal-misconduct, LE, or CI investigation purposes of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, clergy, or psychotherapists and their assistants. Under these circumstances, such communications and work products 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 USG actions for purposes of communications security or network administration, defense, operation, or protection. This includes all communications and data on an IS, regardless of any applicable privilege or confidentiality.
    - The user consents to interception, capture, or seizure of all communications and data for any authorized purpose (including personal-misconduct, LE, or CI investigation when applicable). Giving consent to interception, capture, and seizure of communications and data, however, does not constitute consent to the use of privileged communications or data for personal-misconduct, LE, or CI 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 according to established legal standards and DOD policy. If a user intends to rely on the protections of a privilege or confidentiality, the user is strongly encouraged to seek personal legal counsel on such matters before using a USG IS for that purpose.
    - 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 according to 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 USG 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, as well as the legal protections regarding the use and disclosure of privileged information. Accordingly, such communications and data are private and confidential. Further, the USG shall take all reasonable measures to protect the content of captured, intercepted, and 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 personal-misconduct, LE, or CI investigation purposes (that is, for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, clergy, or psychotherapists and their assistants), the USG may, solely at its discretion and in accordance with DOD policy, elect to apply a privilege on the information or another restriction to the USG's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of a particular IS 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 simply provides a summary of such conditions, and whether the banner expressly references this User Agreement or not.

Part II — Mobile Device User Agreement (Continued)

User Responsibilities for Device and Network Security

This agreement pertains to the end users of permanent- and temporary-issued, unclassified mobile devices (that is, mobile equipment (for example, BlackBerrys, cell phones, smartphones,* tablets, mobile routers) that are combined with an active subscriber-identity-module (SIM) chip).

***NOTE:** A smartphone is defined as a mobile phone built on a mobile operating system (OS).

- The following are general rules governing all users of USG-issued mobile devices:
  - ○ USG-owned hardware and software (including mobile devices) may be used only for official duties.
  - ○ Only authorized individuals will use USG-issued mobile devices.
  - ○ Mobile devices will be removed from the network if the users make any changes to the device that prohibit the Mobile Device Manager (MDM) from properly operating.
  - ○ After 30 calendar days of non-usage, a user's account will be marked as inactive and may be deleted from the MDM.
  - ○ Classified material is not authorized on the mobile device. Users must contact their security manager for all security violations or in the event of any spillage.
    - Devices must be turned off and batteries removed during any classified discussions. If not possible, the device must be placed in an approved designated storage area outside the classified area.
    - Devices will not be used within 3 meters (9 feet) of a Secret Internet Protocol Router (SIPR) workstation.
  - ○ Although Global Positioning System (GPS) features may be available for use on the mobile device, GPS may be used only with approved applications (apps) and must be turned off when those apps are not in use.

NOTE: GPS is a tracking device when it is active. Therefore, users must check with their operations security (OPSEC) officer for guidance on using this feature before traveling, and specifically if traveling outside the United States.

- Additionally, mobile-device users—
  - ○ Will use their mobile devices only according to DOD and local security and wireless policies.
  - ○ Will update their mobile device OS (for example, Android, iOS) only when notified by one of their telephone control officers (TCOs) (Part IV), the IT helpdesk, or the DOD Mobility Program Management Office (PMO), Defense Information system Agency (DISA).
  - ○ Will not install any unauthorized software (including apps) or hardware nor intentionally introduce any malicious code, Trojan-horse programs, unauthorized code, or viruses.
    - The DOD Mobility PMO maintains a list of authorized apps in the DOD Mobile Application Store (MAS) (*https://disa.deps.mil/ext/cop/dod_mobility/SitePages/UserCornerHome.aspx*) for specific devices (that is, at “mobile@works” for Android devices and “P.U.M.A. & DOD Apps” for iOS devices).
    - Downloading third-party apps will result in the user's device being flagged for noncompliance and potential removal from the network.
  - ○ Will not engage in any activity that interferes with the DOD network or any services available on the DOD network.
  - ○ Are not authorized to connect the USG-issued mobile device to any personal or USG computer or laptop.
    - Unapproved connections of the mobile device will result in the user's device being flagged for noncompliance and may result in service suspension.
    - Users must not connect the device to a USG computer using a USB connection, not even to charge the device. On a USG computer, the device will be detected as a storage device and the user's account will be locked.
  - ○ Must adhere to the password complexity policy when setting up (provisioning) the device. This feature must remain enabled. Disabling or not enabling this feature during the set up process will flag the device as noncompliant and the device will be wiped. To be in compliance with DOD policy (that is, the DISA Mobility Security Technical Implementation Guides (STIGs))—
    - All Apple iOS passcodes and Samsung Knox passwords must have at least eight, nonsequential, alphanumeric characters.
    - BlackBerry device passwords must have at least six nonsequential, alphanumeric characters.
  - ○ Must enable WPA2 encryption* when using a DOD mobility unclassified capability (DMUC) device's hotspot capability and change the device name to something that is not meaningful (for example, not an end user's name, a product name, a room number, a site name), change the manufacturer's default hotspot password, and turn off the hotspot when not in use.
    - ***NOTE:** WPA2 cannot be disabled on Apple iOS devices.
  - ○ Who suspect that their mobile device has been compromised must immediately open a trouble ticket with their local IT help desk and contact their security manager. A compromising event may include, but is not limited to, unauthorized password change, a function or feature change, or apps unexpectedly appearing on the mobile device. If compromised, the mobile device may be wiped of its apps and data and the service will be suspended.
  - ○ Are authorized to connect to commercial local-area wireless computing (that is, Wi-Fi) networks only if the network is a trusted Wi-Fi network with WPA2-Personal (also known as, WPA-pre-shared Key (PSK)) security.
    - According to DOD commercial mobile device (CMD) policy (V2R3 STIG, WIR-SPP-010), a trusted commercial Wi-Fi network is defined as a site-managed Wi-Fi access point connected only to the Internet (Internet Gateway Only Connection) or a home Wi-Fi network (user managed).
    - Hotel and other public Wi-Fi hotspots are not considered trusted nor authorized for access.
  - ○ Will not use AirDrop, iCloud Drive, Keychain, or Handoff; share location data through the iCloud; store personally identifiable information (PII) in the Health App; store payment data in Apple Pay; or use a near-field-communications (NFC) radio. These features are not approved for use and must be disabled on all iOS devices. Users are not authorized to enable these features on their devices.

Part II — Mobile Device User Agreement (Continued)

User Responsibilities for Device and Network Security (Continued)

○ Will not use removable media (for example, SD cards, micro-SD cards) on any USG-provided mobile device.

○ Will not transmit PII or any For Official Use Only (FOUO) information to a non-USG-controlled entity.

○ Are not authorized to forward private residence telephone calls to USG-issued mobile devices unless approved by the commander for telework.

○ Are not authorized to forward personal cell-phone calls to USG-issued phones or mobile devices.

○ Are not authorized to add third-party personal e-mail accounts (for example, Google Gmail, Hotmail, Yahoo mail) or to sync contacts or calendar events between public apps and the device. Users may be held responsible for damages caused to USG data or ISs by user negligence or willful acts.

○ Must take the appropriate required actions (Incident Reporting below) when a mobile device is lost or stolen, indicates a computer-network intrusion, or is involved in spillage of classified information.

○ Will physically present their mobile devices and accessories, at least annually, to their local TCO for an inventory review and to sign a new user agreement.

Incident Reporting

Mobile-device users will immediately report—

● Any indication of computer-network intrusion (that is, abnormal operation or behavior), degradation or interruption of wireless-access service, or compromise of data or file-access controls to the Europe Enterprise Service Desk (ESD) (mil 119 or civ 0049-(0) 611-143-523-1000) and follow any incident-response instructions given.

● Spillage of classified information to their organization or unit S2 and the Europe ESD (mil 119 or civ 0049-(0)611-143-523-1000) and follow any instructions given.

● The loss or theft of any mobile devices to their local TCO during duty hours or to the USAREUR TCO (Part IV provides contact information, for example, 0162-270-1702 after duty hours). If a smartphone is lost or stolen, in addition to contacting the issuing TCO, users must also contact the Europe ESD (mil 119 or civ 0049-(0)611-143-523-1000) to turn off the data feature at the server-level and prevent unauthorized e-mail access.

USAREUR Requirements

The use of mobile devices results in high costs to the USG. Management controls over equipment with active SIM chips are therefore required. Users, their supervisors, and the commanders or organization directors of mobile-device users are responsible for ensuring organizational compliance with the following:

● When users are scheduled to deploy, they will return mobile devices to the unit TCO before deploying. Exceptions may be approved by the USAREUR G3/5/7.

● Mobile devices will not be used—

○ For other than official USG business. Personal use is prohibited.

○ As the primary means of communication when the user is on post, in garrison, or in another facility if other USG means of communication that are less costly are available (that is, military (Defense Switched Network (DSN), Sensitive but Unclassified Network (SBU), and Voice-over-Internet-Protocol (VOIP) network) or official-commercial telephones). Users should always use the least expensive means of communication, even during official trips.

○ For health, morale, and welfare calls or personal browsing.

○ For out-of-country (international) calls, unless the time, location, or other circumstances do not permit the use of other telephone services.

○ In areas where prohibited by local law or regulation (for example, some healthcare facilities).

● Wireless devices are prohibited from being brought into any Army or DOD secure vaults, sensitive compartmented information facilities (SCIFs), secure-teleconference or video-teleconference rooms, and any other areas where classified information is discussed, stored, processed, or transmitted.

● Users are prohibited from using USG-issued mobile devices while driving, unless a hands-free feature is installed in and part of the vehicle (Bluetooth devices are permitted with class 2 or 3 mobile devices operating Bluetooth version 2.0 or later). Additionally, any form of SMS texting is prohibited while driving.

● Users will be held liable for the cost and roaming charges for personal calls initiated or received outside their geographic area of service coverage.

● Users will be held liable for any unauthorized calls made on an assigned mobile device, even if the call was made by another individual. The user must be aware of additional costs, such as roaming fees or the cost for downloading attachments.

● Personal- and USG-owned mobile devices are prohibited from connecting to DOD workstations.

● When a user prepares to depart a unit or position, the user must return the mobile device to the issuing (usually, the unit-level) TCO. The user will not pass the device to another individual.

Print Form | E-mail Form | Reset Form

Go to page 1 2 3

Part III — Special Instructions

Part IV — POC Information

● The primary POC for this agreement is either the equipment-issuing unit TCO or the applicable master TCO (that is, the unit senior TCO who has billing-detail viewing authority), as appropriate according to the unit and USAREUR major subordinate command local policy.

● To report problems or ask questions, the user should always first try to contact the organization or unit TCO:

○ Organization or unit TCO (rank Name): _____

Military _____ or civilian _____

○ USAREUR TCO (HQ USAREUR and subordinate units):

Military 314-537-6666 or civilian 0049-(0)611-143-537-6666

○ Theater Enterprise TCO (5th Sig Cmd):

Military 314-565-0334 or civilian 0049-(0)611-143-565-0334 and 0049-0162-273-1011 (after duty-hours)

○ Europe Enterprise Service Desk (ESD):

Military 119 or civilian 0049-(0)611-143-523-1000

Part V — Equipment Data

Device information (Select the type of mobile device.)

☐ Cell phone ☐ Electronic tablet or iPad ☐ AirCard (mobile hotspot) ☐ MiFi hotspot (mobile Wi-Fi router) ☐ Smartphone

SIM card number	Telephone number	Personal identification number (PIN)	Personal unblocking key (PUK)

Device model	Device international mobile station equipment identity (IMEI)	Device Wi-Fi media-access-control (MAC) address (MobileIron devices only)

Customer job-order number	Apple ID	Password	Passcode

Part VI — User Agreement

By signing this user agreement, I acknowledge that I accept and will abide by all the above terms and conditions and verify that I have updated my personal information (Part I) and confirmed the information (Part VI) for the mobile device.

Type or printed name (First MI. Last)	**Date** (YYYYMMDD)	**Signature**

Part VII — TCO Verification and Issue Information

The signed original of this form will be kept on file by the issuing (unit- or higher-level) TCO according to local organization or unit policy. The issuing TCO will give the user a copy.

Equipment issued

Type or printed name (First MI. Last)	**Date** (YYYYMMDD)	**Signature**

Equipment Turned In

Type or printed name (First MI. Last)	**Date** (YYYYMMDD)	**Signature**