MOBILE COMPUTING DEVICE USE

For use of this form, see AR 25-2 and DIACAP Controls ECSC, ECCR, ECWN, ECCT, ECML, and ECVP

1. SCOPE. This policy applies to all Soldiers, civilians, and contractors who use a Mobile Computing Device (MCD) that is supported and serviced by the Fort Knox Network Enterprise Center (NEC). The scope of this document includes the Fort Knox Installation Campus Area Network (FKICAN), sensitive but unclassified (SBU) internet protocol router network, laptops, portable notebooks, tablet-PCs, and similar systems referred to as MCDs which pose security challenges. This does NOT apply to two-way electronic data-retrieval devices such as BlackBerry, two-way text messaging devices, pagers, cell phones, or similar technologies.

2. USER RESPONSIBILITIES. All users are tasked with the physical security of MCDs, whether they are a stand alone system or connected to the FKICAN. As an MCD user, I will adhere to the following:

a. I will notify my information management officer (IMO) to coordinate any requirements at least 2 working days, if possible, prior to removing an MCD from the installation. My IMO will coordinate with the NEC IT specialist if any issues arise.

b. I will test the virtual private network (VPN) connection and ensure I can access those programs required when the MCD is away from Fort Knox. This will ensure I can log on and connect as if I am TDY.

c. Upon return from travel, I will notify my IMO when the MCD is returned to Fort Knox.

d. I will remove peripheral devices and removable cards when not in use, as these devices consume battery power and contribute to heat levels within the MCD. I will secure these items to prevent damage, loss, or theft.

e. I will maintain the MCD serial and model identification numbers, computer name, and emergency point of contact information separately from the MCD while traveling (i.e., wallet or suitcase).

f. I will be responsible for ensuring my common access card (CAC) credentials are valid for the length of time the MCD is disconnected from the FKICAN.

g. I will include a business card or similar identifier affixed to the MCD or in the carrying bag.

h. I will secure the MCD at all times when not in use and in my possession.

(1) Car Rental/Privately-Owned Vehicle Travel. I will never leave the MCD in a vehicle where it can be seen. If possible, I will use a cable lock to secure it to a permanent vehicle mount. If possible, I will choose a rental car with an alarm system and no external rental identification stickers. I will keep in mind that extreme temperature ranges inside an unattended vehicle could easily destroy the MCD.

(2) Hotels. I will never leave the MCD unsecured in a hotel room. If I have a cable lock for the MCD, I will anchor it to a fixed object. If I do not have a cable lock, I will secure it in a room safe, and if nothing is available to secure the MCD, I will take it with me.

(3) Air/Rail Travel. I will never place an MCD in checked or unattended baggage. I will keep the MCD in sight at all times, especially through security checkpoints. If possible, I will send the MCD through a security checkpoint when the exit is free of previous travelers. I will be vigilant in any circumstances where there is a sudden diversion involving me or another person in my vicinity, especially at security checkpoints. I will use a non-descript carrying case and will not publicly display an MCD case highlighting manufacturer, organization, military affiliation, or company's logo on the side. I will secure or lock the zippers of my case so no one can reach into the bag and remove the MCD.

(4) Meetings/Conferences. I will never leave the MCD unattended in public meetings, conventions, or conferences.

i. I will never download and install software applications or enable unauthorized protocols or services.

j. I will ensure a backup of any MCD data before departing on TDY and secure the backup at my normal duty station.

k. I will not connect to more than one active interface at a time (i.e., do not connect to a wireless network and government-wired connection at the same time or to a modem and government-wired connection at the same time).

l. I will avoid using MCDs in areas where "shoulder surfing" is easy.

m. When the MCD is off the installation, I will use the Fort Knox VPN/Outlook web access connection, when available, for accessing the internet or checking e-mail.

n. I will ensure all personally identifiable information (PII) and For Official Use Only (FOUO) information is secured in an encrypted folder on the MCD hard drive. I will encrypt folders instead of individual files so that if a program creates temporary files during editing, they will be encrypted. Information identified as sensitive (formerly SBU) will be encrypted and signed before e-mail transmission. (NOTE: Encryption may double the original size of an e-mail, depending on the specific encryption algorithm used, consuming additional bandwidth and causing network delays.) If data cannot be encrypted before transmission or the unencrypted file size is greater than 2 megabytes, the data must be uploaded to a PK-enabled website (i.e., AKO) that is only accessible by the intended recipient(s). I will inform users where to access data on the PK-enabled website instead of transmitting the content. The following categories are information that should be encrypted:

(1) For Official Use Only (FOUO). In accordance with (IAW) AR 25-55, The Department of the Army Freedom of Information Act Program, 1 November 1997, FOUO information is information that may be withheld from mandatory public disclosure under the Freedom of Information Act (FOIA).

(2) Unclassified Technical Data. Unclassified technical data is data related to military or dual-use technology that is subject to approval, licenses, or authorization under the Army Export Control Act and withheld from public disclosure IAW DOD 5230.25.

(3) Department of State (DOS) SBU. The DOS SBU is information originating from the DOS that has been determined to be SBU under appropriate DOS information security policies.

(4) Foreign Government Information. Foreign Government Information is information originating from a foreign government that is not classified CONFIDENTIAL or higher but must be protected IAW DOD 5200.1.

For a listing of examples, see Appendix A of the Army's Best Business Practice Data-At-Rest (DAR) Protection, 06-EC-O-0008.

o. I will ensure a firewall and anti-virus software are used and up to date when not connected to the FKICAN. This is set as part of the NEC baseline for MCDs.

p. I will not use Bluetooth technology/devices with Government equipment. Wireless peripheral devices such as keyboard, mice, printers, etc., are not authorized.

q. I will scan all media (i.e., diskette, CD-ROM, USB drives, etc.,) before accessing it.

r. I will not transport any MCDs with radio frequency/wireless, infrared, Bluetooth, and audio/video record capable wireless devices in an area where classified information is discussed or processed and will not connect to any classified networks. These devices will not be used for storing, processing, or transmitting classified information.

s. When not in use, I will turn off/disable the wireless device if my MCD has one.

t. I will immediately report loss of the MCD to my IASO/IMO or NEC Customer Support Center (502-624-8888), my commander/director, and law enforcement representatives, regardless of the type of information contained on the MCD.

u. I will always log off and shut down the MCD during travel and will never use sleep or hibernation modes.

v. While away from the installation, I will ensure the MCD is connected to the FKICAN at least once a week and long enough to receive required updates and security patches.

w. I will ensure Split tunneling is disabled on the VPN Client (i.e., Upon establishment of a VPN connection to a DOD network, no other connections of any kind will be established (e.g., If home networks are used, no connection between the device and other home network devices will be established during a VPN session.))

x. I will only access DOD networks from approved Government furnished equipment or contract systems approved and accredited for use on a Government network and use this to access Army ISs (computers, systems, and networks) for authorized purposes.

3. INFORMATION MANAGEMENT OFFICER (IMO) RESPONSIBILITIES.

a. The IMO will notify the NEC IA office, via e-mail notification, of the MCD's return to Fort Knox and request a scan. The NEC IA office will scan the MCD and notify the NEC IT specialist if any updates are required.

b. The IMO will ensure all unclassified MCDs are properly labeled with a US Government SF710, Unclassified (Label), affixed in clear view; FK Label 1015-E, This Equipment Will Not Be Used To Process Classified Material; and FK Label 5078, Data-At-Rest Laptop Label.

c. When a user notifies the IASO/IMO of a lost or stolen MCD, the IASO/IMO will immediately notify the Installation IAM. If the event occurs during the weekend or at night, the IMO will contact the Installation Operations Center (IOC) at (502) 624-5151. The IOC will contact NEC.

d. The IASO/IMO will verify the MCD has approved FKICAN baseline, properly named, appropriately labeled (PII, DAR, inventory, unclassified, etc.,), CAC enabled/enforced; ensure current Retina scan with all CATs 1 and 2 vulnerabilities are mitigated; ensure only approved and accredited software is loaded, the guest account has been changed, password protected, and disabled; and ensure the local administrator name has been changed/password protected, all audit logs are enabled and max log size is no less than 2,048 KB and the overwrite events, as needed, is activated. The IASO/IMO will also verify approved antivirus has been loaded, AV signature is up to date, and password protected screen save is set IAW AR 25-2.

I HAVE READ AND UNDERSTAND THE ABOVE PROCEDURES REGARDING USE OF MCDs; I WILL FOLLOW THE PROCEDURES OUTLINED AND PROPERLY SAFEGUARD THE EQUIPMENT AND DATA.

USER LAST NAME, FIRST NAME, MI:	PHONE NUMBER:	ORGANIZATION:

USER SIGNATURE:	DATE:

THE USER HAS COMPLETED AND WILL MAINTAIN PII AWARENESS AND DOD IA AWARENESS TRAINING REQUIREMENTS IAW DOD 8570.1 AND AR 25-2. THIS USER HAS A CURRENT, UP TO DATE, AND SIGNED COPY OF THE FKICAN ACCEPTABLE USE POLICY ON FILE WITH THE UNIT IASO/IMO.

IASO/IMO SIGNATURE:	DATE: