UNCLASSIFIED / FOR OFFICIAL USE ONLY
SNET MOBILE DEVICE USER AGREEMENT

PRIVACY ACT STATEMENT

Disclosure of this information is voluntary. However, non-disclosure will result in denial of ***Mobile Device*** system access. Authority to request this information is contained in 5 USC Section 301 for the purpose of requesting information to ensure that all SNET military, civilian, and contractor personnel who have signed this security briefing/user agreement form are correctly identified. Also 10 USC Part II and 14 USC Chapter 11 provide authority for the Command Information Systems Security Manager (ISSM) to use the above data to ensure proper security indoctrination of all assigned personnel.

PART I - PERSONAL INFORMATION

1. LAST NAME	2. FIRST NAME	3. RANK/GRADE
4. ORGANIZATION	5. SNET PHONE NUMBER	6. UNCLASSIFIED EMAIL ADDRESS

PART II – ACKNOWLEDGE AND CONSENT

Per DoD Chief Information Officer Policy, the following acknowledgement 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 Special Operations Command Europe (SOCEUR) information systems:

You are accessing a SOCEUR 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 J6X 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, SOCEUR 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. and Partner Nations 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.

PART II – ACKNOWLEDGE AND CONSENT (Continued)

- 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. 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.

(U) PART III - SECURITY REQUIREMENTS

The following preventive measures are requirements to ensure that use of the Mobile Device does not result in the release of DoD information to unauthorized persons.

- I acknowledge that the device provided is not my personal property. I shall not modify applications, configurations, or use outside the scope of intended purpose/official duties. Further, I will not download any application (i.e. “apps”) or software without prior approval from the SNET Tier 1 Administrator. Improper use or modification of this device may result in a security violation for which I may be subject to punitive, disciplinary, criminal, or adverse administrative action.

- I acknowledge that this device will not be used for transmission of classified data. .

- I agree to log out or lock the device when it is not being used and not to allow the device to be unattended while logged in.

- I am aware of my responsibility to regularly verify the physical integrity of the mobile device and to check for evidence of tampering. I acknowledge that if the device appears to have been tampered with, or the device otherwise malfunctions, I am not to use the device or try to fix it. I will not contact a commercial vendor to troubleshoot or exchange.

- I acknowledge my responsibility to immediately report the loss, theft, unauthorized use, and/or tampering of the device to my Command and/or SNET Tier 1 Administrator.

- I agree to make the device available to the SNET Tier 1 Administrator for a hands-on/visual inspection of the device, periodic audits, and update verification.

- I understand that I may permit mobile devices to be physically/visually examined at installation entry points, airports, and other similar locations where computing equipment is routinely inspected, and may power it on upon request. I understand that I may put the device through an x-ray machine, but that I may not surrender the device to another individual to be checked outside of my control/sight. I also understand the procedure to follow if asked to display information or surrender the device.

- I understand that mobile devices with wireless capability cannot be taken into a SCIF or non-SCIF Classified Data Processing Area unless approved by the SSO.

(U) PART IV – SECURITY REQUIREMENTS (Continued)

- All actions may be monitored, including: Internet use, e-mail, installed applications, and geo-location. Misuse may result in access termination and/or subject me to appropriate punitive, disciplinary, criminal, or adverse administrative action.
- While I may use this device for limited personal use provided that such use does not overburden the system or result in additional unapproved cost to the government, I understand that any/all personal correspondence from the device may be monitored.
- I shall not transfer or provide this device for unattended use to others; it is my responsibility to ensure any person using the mobile device (in my presence) is properly cleared for use.
- I will not sync any device to a rental car (direct or wireless connection), or use any type of public USB charging I will not accept/borrow/use an extended charging device or cable not issued by my command.
- I have receive the acceptable use training from my Commands SNET Tier 2 Administrator.

FOR REPORTING PROBLEMS, INCIDENT HANDLING OR TO ASK QUESTIONS, CONTACT YOUR SNET TIER 1 ADMINISTRATOR

By signing this user agreement, I acknowledge that I accept and will abide by all the terms and conditions described above.

12. NAME OF WHO CODUCEDT AUP TRAINING	13. TRAINING DATE
14. SIGNATURE OF USER	15. DATE SIGNED (YYYYMMDD)