UNCLASSIFIED / FOUO

DECTK-GW USER AGREEMENT (Version 3.6)

NOTE: This information may be used to contact a DECTK-GW user in the event of a security incident or an emergency.

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the user of the DoD Enterprise Classified Travel Kit Gateway (DECTK-GW) device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security and wireless policies. This information is used for inventory control of the device and to verify compliance with DoD requirements regarding accountability of classified information and COMSEC material, and provides user emergency contact information in the event that the device is lost, stolen, otherwise compromised, or requires a reconfiguration due to security policy changes. ROUTINE USE(S): None. DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial of issuance of a DECTK-GW device.

PART I - PERSONAL INFORMATION

1. LAST NAME	2. FIRST NAME	3. RANK/GRADE
4. ORGANIZATION	5. MAILING ADDRESS	6. CITY/STATE
7. COMM TELEPHONE #	8. DSN TELEPHONE NUMBER	9. ALTERNATIVE TELEPHONE NUMBER

10. NIPR E-MAIL ADDRESS

SIPR E-MAIL ADDRESS

PART II - DECTK-GW INFORMATION

11. The following preventive measures are requirements to ensure that use of the DECTK-GW device does not result in the release of DoD information to unauthorized persons.

(U//FOUO) I have been issued a DoD Enterprise Classified Travel Kit Gateway (DECTK-GW) device. As such, I agree to abide by the United States Government rules and regulations carried in Joint Ethics Regulation, DOD 5500.7-R as they apply to my use of this U.S. Government device. In addition, I acknowledge and consent to the terms carried in the "Notice and Consent Provision" (ANNEX A of this User Agreement).

(U//FOUO) I acknowledge that I have read, understand and agree to comply with the restrictions and requirements set forth in this agreement and ANNEX A. I acknowledge that intentional violation of these terms may result in seizure of my DECTK-GW device and/or adverse administrative action.

(U//FOUO) I understand and agree to the following:

a. I have an active SECRET clearance and must maintain this clearance as long as this device is assigned to me. If my Secret clearance is revoked after I have been issued this device, I will immediately return the device to my organization's authorized representative, in accordance with my organization's established security procedures.

b. The device is only approved for use up to SECRET voice/data (e.g., e-mail, Web browsing) and at no time may it be used for any Top Secret (TS)/ Sensitive Compartmented Information (SCI) communications.

c. Any voice, video or data communications utilizing the gateway/network shall not exceed the SECRET level.

d. Processing classified information at a level higher than designated for the device could lead to a compromise of classified information. Such processing is prohibited, constitutes a security violation, and could lead to administrative action, seizure of the device, and/or referral to the appropriate law enforcement authorities.

e. User storage of classified data on the device is strictly prohibited and shall be considered spillage; improper device use protocols will apply.

f. The device is unclassified and high value until it is provisioned (keyed), booted (powered on) and the user password is authenticated. Upon user password authentication, the device is classified and must be handled at the highest level of the key activated on the device. It will also be considered classified at all times if there is a laptop.

g. I shall remove the cryptographic key when not in an active call, reviewing email, or conducting a secure Web browsing session.

h. The User shall obtain their organization's Authority to Operate (ATO). Even if the kit does not plug into a government internet port, it still reaches back to a government enclave. Therefore, your organization must have

an ATO from your DAA/AO.

i. I must maintain continuous physical control of the device or keep it stored in a manner that will minimize the possibility of loss, theft, unauthorized use, or tampering. Secure storage may be a user-controlled compartment with a lock and key (e.g., a desk drawer, cabinet, motor vehicle, or the user's residence.).

j. I will use the device in classified mode with minimal risk of compromise of classified information. I shall maintain an awareness of my surroundings and proximity to uncleared personnel who may be privy to voice or text conversations.

k. I will not use the device when I have access to a SIPRNet LAN.

l. I will not use the device in possibly unsecure OCONUS residence or hotel locations.

m. If the device cannot remain in my physical control, I shall power it off and secure it in a limited access location.

n. In instances where the device is out of my physical line of sight, I shall inspect the device for signs of tampering when I regain physical control of it. Suspected unauthorized use or tampering must be immediately reported to DECTK support; the device will immediately be removed from the network.

o. When a device is reported lost, damaged, or improperly destroyed, the incident shall be reported to the **DISN Customer Contact Center (DCCC) at DSN 312-770-9500 or Toll Free 1-855-868-9500** and investigated immediately in accordance with local organizational accountability procedures. DECTK-GW devices are government property and accountable devices. In the event of damage (other than fair wear and tear), negligence or abuse, please follow your internal organization procedures for property accountability.

p. Should I wish to permanently relinquish the device, I will contact DECTK-GW support for de-boarding.

q. I agree to comply with DECTK-GW property accountability procedures, including periodic auditing deemed necessary by the PMO to verify continuing possession of DECTK-GW equipment. This includes but is not limited to periodic re-provisioning of the kit, updated user agreements and POC information.

s. Introducing the device into a secure facility shall be subject to controls established by the presiding security authority. I am responsible for awareness and compliance with local facility security controls and procedures. Prior to bringing the device into a U.S. Government area secured higher than SECRET, the device must be powered off.

t. Connecting the device to any classified or unclassified information system within any Sensitive Compartmentalized Information Facility (SCIF), except by the authorized system administrator for the purpose of provisioning the device is strictly prohibited.

u. The user agrees to adhere to their service/agency Physical Security, COMSEC, and Information Assurance policy.

v. User kits will be current with DoD STIG (Security Technical Implementation Guideline). User will accept responsibility for any security violation involving their approved kit(s).

(U//FOUO) I affirm my completion of all required user training, including instruction on proper use and protection of the device and its security features.

(ANNEX)

DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," 9 May 2008 Requirements:
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, (Le., 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.

12. SIGNATURE OF USER	13. DATE SIGNED (YYYYMMDD)