US AIR FORCE UNCLASSIFIED WIRELESS MOBILE DEVICE USER AGREEMENT

The policy described in this memorandum is in accordance with the Air Force Instruction (AFI) 10-712, Telecommunications Monitoring and Assessment Program (TMAP); AFI 33-100, User Responsibilities and Guidance for Information Systems; AFI 23-111, Management of Government Property in Possession of the Air Force; AFI 33-200, Information Assurance (IA) Management, DTM-08-060, Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement; Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).

AUTHORIZED USE/ACCESS TYPE: *End-user exclusively.*

PART I - PERSONAL INFORMATION *(To be completed by End User)*

1. LAST NAME	2. FIRST NAME	3. RANK/GRADE
Gardiner	Joshua	Contractor
4. ORGANIZATION	**5. TELEPHONE NUMBER**	**6. WORK E-MAIL ADDRESS**
Knowledge Management	318-456-4565	joshua.gardiner.ctr@us.af.mil

PART II - WIRELESS/PORTABLE ELECTRONIC DEVICE INFORMATION

If multiple wireless devices are assigned to an individual or shared by multiple users, document all devices in Block 12 or on another locally created sheet and affix to this user agreement. Only one wireless user agreement is required to be signed given all devices are appropriately documented.

7. DEVICE TYPE	8. DEVICE MODEL	9. DEVICE TELEPHONE NUMBER	10. SERIAL NUMBER
LAPTOP	HP	N/A	MXL65021P4

11. ORGANIZATION DEFINED REQUIREMENTS *(e.g., CAC Sled Serial #, International Mobile Equipment Identity (IMEI)/International Mobile Equipment Identifier (MEID), Common Access Card (CAC) and Subscriber Identification Module (SIM), etc.)*

N/A

12. REMARKS AS NEEDED

Device Name: AWUBL-GA5021P4

PART III - ACKNOWLEDGEMENT 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 Department of Defense (DoD) information systems:

1. 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.

2. You consent to the following conditions:

   a. 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.

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

   c. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, search, and may be disclosed or used for any U.S. Government-authorized purpose.

   d. 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.

   e. 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:

      (1) 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.

      (2) 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

f. 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.

g. 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.

PART IV - SECURITY REQUIREMENTS

The following preventive measures are required to ensure that use of wireless devices do not result in release of DoD information to unauthorized persons.

1. I understand that this wireless device is provided for official U.S. Government and authorized use exclusively. Only authorized information may be stored on or transmitted by this device. Misuse of this device (use outside of official U.S. Government and authorized purposes) may subject me to appropriate administrative, disciplinary, criminal, or other adverse actions.

2. I am the only individual authorized to use the wireless device. I am responsible for physical damage to the device and the confidentiality and integrity of data on the device. Any damage caused will be immediately reported to my organizational Information Assurance Officer (IAO).

3. I understand that if this device is lost or stolen, I must immediately report it to the Service Desk and my organizational IAO.

4. I understand the wireless device will be technologically (logical access) and physically secured. I will maintain device accountability at all times.

5. I agree to follow all wireless remote access responsibilities, security measures/requirements, and annual wireless training requirements identified in Air Force policy and applicable DISA STIGs.

6. I understand that if I notice unusual activity, malfunctions, or abnormalities of this device; I will immediately report and return the device to the Service Desk or my organizational IAO. I will not use or attempt to fix the device as it may have been compromised.

7. I understand that I will not connect this device to other computing equipment, including personal laptops (e.g., tethering or wireless personal area network [WPAN], air card use, and device synchronization [hot-synch]) without prior Designated Accrediting Authority (DAA) approval. I will also observe device-specific stipulations prior to any connections. I will not exceed my authorized user access and enable unauthorized functionality of this device. I will follow any local Wireless Remote Access connection policies and approval procedures prior to use.

8. If issued a Smartphone device and Wi-Fi access is authorized, I will follow local command connection policies and conditions governing when and where the smart phone device may be connected to Wi-Fi access not controlled by DoD.

9. I understand that wireless devices connected directly to a DoD-wired network (e.g., via a hot synch connection to a workstation or connected via RJ-45) are not permitted simultaneous wireless operation. I will not configure the device to function as ad hoc wireless access point to connect other wireless devices to the DoD-wired network.

10. I understand wireless devices are not approved for handling/storing sensitive information unless properly encrypted.

11. I understand that I must exercise discretion (operations security) at all times when using government issued wireless devices. During use, I will position this wireless device display to prevent the inadvertent disclosure of viewed information by unauthorized users.

12. I understand when transferring sensitive DoD information with this wireless device, I must sign and encrypt messages using DoD Public Key Infrastructure (PKI) credentials.

13. I acknowledge that wireless devices with digital cameras (still and video) are not allowed in any Sensitive Compartmented Information Facility (SCIF) or other areas where classified documents or information is transmitted, received, stored, or processed.

14. I understand that this wireless device is not secure and will not be used to transmit, receive, store, or process classified information.

15. I understand that if classified information is inadvertently sent, accessed, or stored on this device, I must immediately turn off and/or remove the battery from the device and contact the Service Desk and my organizational IAO to report as a data spill incident.

I acknowledge I will not use this wireless device within 3 meters (9.8ft) of any classified environment/dat equipment unless authorized by the DAA. I understand additional local restrictions may be required.

17. I will not configure wireless devices to download, install, or use unauthorized applications, software updates, or personal e-mail accounts (e.g., AOL, Yahoo, Gmail, etc.) unless authorized by the DAA.

18. I acknowledge that only authorized wireless peripherals and Bluetooth devices (including CAC readers, and headsets/hands free devices) will be used/ synchronized to this wireless device and I must contact the Service Desk and/or my organizational IAO for a list of approved devices.

19. I acknowledge that messaging applications (Short Message Service (SMS) and Multimedia Messaging Service (MMS), or similar capabilities) are provided only to individuals who have been granted approval by the DAA or his/her assigned representative. Information exchanged between devices using messaging applications is not authorized for the transmission, receipt, storing, or processing of Controlled Unclassified Information (CUI), FOUO information), Privacy Act (PA) information, and Personally Identifiable Information (PII).

20. I understand locally created operating instructions on use of wireless devices may accompany this user agreement.

21. I acknowledge receipt of and responsibility IAW AFI 23-111 for the items described and will return the device when no longer needed.

FOR REPORTING PROBLEMS, INCIDENT HANDLING OR TO ASK QUESTIONS, CONTACT THE ORGANIZATIONAL IAO OR SERVICE DESK

By signing this User Agreement, I am acknowledging that I accept and will abide by all the terms and conditions described above.

13. DATE SIGNED (YYYYMMDD)	**14. SIGNATURE OF USER**
20201015	Joshua Gardiner Digitally signed by Joshua Gardiner Date: 2020.10.15 11:45:54 -05'00'

NOTE: This signed Unclasified Wireless Mobile Device User Agreement will be retained by the Organizational IAO or the designated representative for a a minimum of six months after the device has been returned to the issuing office.