DEPARTMENT OF THE AIR FORCE (DAF) USER AGREEMENT STATEMENT - NOTICE AND CONSENT PROVISION

AUTHORITY: Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*; Air Force Instruction AFI 10-701, *Operations Security (OPSEC);* Department of the Air Force Manual (DAFMAN) 17-1301, *Computer Security (COMPUSEC)*; DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*; DoDI 5000.64_DAFI 23-111, *Accountability and Management of DoD Equipment and Other Accountable Property;* AFI 17-130, *Cybersecurity Program Management*.

PRINCIPAL PURPOSE: To ensure users are made aware of, and consent to, Department of Defense (DoD) and Department of the Air Force (DAF) monitoring policies and procedures.

ROUTINE USES: May be disclosed for the purpose of verifying individuals were made aware of monitoring policies and procedures. The DoD's Blanket Routine uses for law enforcement and similar purposes apply.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of this request. This form requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized Department of Defense Instruction (DoDI) 5400.11, *DoD Privacy and Civil Liberties Programs*.

PRESCRIBED BY: DAFMAN 17-1301, *Computer Security (COMPUSEC).*

1. NAME (Last, First, Middle)	2. STATUS
	Military ○ Civilian ○ Contractor ◉
3. USER SIGNATURE	**4. DATE (YYYYMMDD)**

By signing this document, you acknowledge and consent that when you access 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, law enforcement, and counterintelligence 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, (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.

The following statements reflect behavioral norms and mandatory standards of acceptable use of DAF Information Technology. By signing below, you indicate both your understanding of these standards and your agreement to act in accordance with them as a condition of your service with or access to systems within the DAF. Air Force Instruction 17-130, *Cybersecurity Program Management*, applies.

1. **I WILL adhere to and actively support all legal, regulatory, and command requirements.**
   a. I understand that DAF Information Technology is used primarily for Official/Government Business and that limited personal use must be of reasonable duration and frequency, that has been approved by my supervisor and does not adversely affect the performance of official duties, overburden systems, or reflect adversely on the DAF or the DoD.
   b. I will not use my access to government information or resources for private gain.
   c. I waive my expectation of privacy in my DAF electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains.
   d. I will observe all software license agreements and Federal copyright laws.
   e. I will encrypt sign any message containing Controlled Unclassified Information or Personally Identifiable Information.
   f. I will promptly report all security incidents in accordance with DAF policy.
2. **I WILL use the system in a manner that protects information confidentiality, integrity, and availability.**
   a. I will not store or process classified information on any system not approved for classified processing.
   b. I will protect my Common Access Card/hardware token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.
   c. I will protect my passwords/Personal Identification Numbers from disclosure. I will not post or write these down in my workspace.
   d. I will lock or log off my computer or terminal any time I walk away.
   e. I understand that my password/Personal Identification Numbers must adhere to current DAF standards for length, key space, and aging requirements.
   f. I will not disclose any non-public DAF or DoD information to unauthorized individuals.
   g. I understand that everything done using my Common Access Card/hardware token/password/Personal Identification Number will be regarded as having been done by me.
   h. I will ensure that anti-malware software is active and up to date on DAF IT assets entrusted to me, and I will immediately notify my CFP or WCO if I believe the assets have been compromised.
3. **I WILL protect the physical integrity of computing resources entrusted to my custody or use.**
   a. I will protect DAF Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.
   b. I will protect DAF Information Technology from tampering, theft or loss. I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.
   c. I will protect DAF Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of the information contained and practice proper labeling procedures.
   d. I will not allow anyone to enter DoD or DAF facilities without proper authorization.
   e. I will not install, relocate, modify, or remove any DAF Information Technology without proper approval.
4. **I WILL NOT attempt to exceed my authorized privileges.**
   a. I will not access, research, or change any account, file, record, or application not required to perform my job.
   b. I will not modify the operating system configuration on DAF Information Technology without proper approval.
   c. I will not move equipment, add, or exchange system components without authorization by my local systems manager or local hardware custodial personnel.
   d. I will not use or connect to non-official hardware, software, or networks for official business without proper approval and without the use of authorized mobile device network encryption.
5. **I WILL NOT use systems in a way that brings discredit on DAF users or the DAF or degrade DAF missions.**
   a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.
   b. I will not receive or send inappropriate material using my official email or Internet accounts.
   c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral, or philosophical agenda.
   d. I will not add slogans, quotes, or other personalization to an official signature block.
   e. I will not access, download, coordinate, or create pornography, sexually explicit or sexually oriented material, nudity, hate speech, or ridicule of others on the basis of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin)

gambling, illegal weapons, militant, extremist, or terrorist activities.

f. I will not use government systems to gamble; pursue illegal weapons; or engage in terrorist unprotected extremist activity.

g. I will not connect or remove any form of removable media without proper approval.

6. I WILL NOT waste system and network resources.

a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook, Twitter, Instagram, Snapchat, TikTok, etc.)

b. I will not make excessive use of my official computer for shopping or to view full-motion videos from non-official sources (e.g., YouTube, online multiplayer video games, etc.)

c. I will not auto-forward email from my official account to a personal email account.

7. I WILL NOT place DoD information into third-party systems.

a. I understand that I am prohibited from placing any DoD information not explicitly cleared for public release into non-DoD controlled information systems, including but not limited to free conference call solutions and agile software development tools, as well as collaboration platforms and artificial intelligence applications (e.g., ChatGPT, Google Gemini, Microsoft Copilot).

b. I acknowledge that compliance with this policy is critical to safeguarding sensitive information and maintaining the integrity of DoD operations, as outlined in AFI 35-101, Public Affairs Operations, and DoDI5200.48_DAFI16-1403, *Controlled Unclassified Information (CUI)*.