TRANSPORT.MIL
USER RULES OF BEHAVIOR/USER AGREEMENT
FOR COMMERCIAL CARRIERS

STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that you are accessing a Department of Defense (DOD) information system (which includes any peripheral devices attached to that information system) and that this system is provided for official U.S. Government use only.

All users acknowledge and consent to the following conditions:

1. 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.
2. At any time, the U.S. Government may inspect and seize data stored on this information system.
3. 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.
4. This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—they are not for personal benefit.
5. 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 products) that are related to personal representation or services by attorneys, psychotherapists, or clergy. The following applies to communications and data (including work products) under these circumstances:
   a. 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, defense, or for COMSEC purposes. This includes all communications and data on the information system, regardless of any applicable privilege or confidentiality.

   b. 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).

   c. 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.

   d. 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 Federal law 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.

   e. Users are to take reasonable steps to identify such communications or data 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 release is otherwise authorized by Statute.

6. In cases when the user has consented to searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative purposes, (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.
7. 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 (hereon referred to as the "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.

System Security Rules of Behavior/Acceptable Use Policy (AUP)

All users shall:

1. Comply with United States Department of Defense External Certification Authority (ECA) X.509 Certificate Policy, latest version.
2. Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know.
3. Assume only those roles and privileges within the application for which they are authorized.
4. Protect information and system resources against occurrences of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse or release to unauthorized persons.
5. Conform to DOD prohibitions on password sharing. Sharing of ECA certificates and or passwords with anyone except to whom it was issued to is a security violation and is cause for immediate suspension of GOPAX account and grounds for revocation of ECA certificate. Specifically, DOD ECA X.509 Certificate Policy, Section 4.9.1. states certificates shall be revoked when the private key is suspected of compromise. **Do NOT share passwords!**
6. Protect password(s) and/or ECA certificate(s), and personal identification number (PIN). Immediately notify their respective organizational security office, and/or ECA issuing authority if they believe their password/PIN has been compromised.

   Policy for ECA certificate violations:

   - First violation: Written warning to the individual from the functional manager with notice to the company and GOPAX Program Manager (PM). Users will also be required to obtain a new certificate at their own expense
   - Second violation: 90-day individual account suspension by the functional manager with notice to the company and GOPAX PM. Users will be required to obtain a new certificate at their own expense
   - Third violation: 1-year removal of the company from the DOD bus and/or air program
7. Not attempt to bypass, strain, or test system information assurance (IA) mechanisms.
8. Not introduce or use unauthorized software, firmware, or hardware on any DOD information system or enclave.
9. Understand that system use constitutes consent to monitoring, recording and auditing.

Transport.mil System Specific Security Rules of Behavior

Transport.mil users shall comply with all other applicable provisions of this document and:

1. Are responsible for protecting all Transport.mil data that they are able to access.
2. Are not authorized to release or share data contained in Transport.mil without the express written consent of the Transport.mil PMO and data owner.
   a. If authorization to release or share data is granted by the Transport.mil PMO and the data owner, it is the responsibility of the user to ensure the recipient of the data has the appropriate background investigation and/or clearance for the data and to establish the recipient has a valid "need to know".
   b. It is the responsibility of the user to provide the Transport.mil PMO with documentation identifying the recipient(s) and the frequency of the release.
   c. The user providing the data assumes all responsibility for the secure transmission of the data released and its protection from unauthorized disclosure.
   d. The user providing the data is responsible to ensure that the recipient(s) purge the data when that data is no longer required.
3. Shall notify the Transport.mil Helpdesk when access to Transport.mil data and/or specific Transport.mil capabilities is no longer required (e.g., reassignment, completion of project, transfer, retirement, and resignation).
4. Are not permitted multiple, concurrent logon sessions.
5. Shall close their browser after logging out of Transport.mil.

Transport.mil Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP)

Transport.mil users may be granted access to personal information about an individual that identifies links, relates to, is unique to, or describes him or her. Examples of this type of data include: social security number, age, rank/grade, marital status, race, salary, medical information, personal home/cell phone number or complete personal bank account number. These types of information are known as personally identifiable information (PII).

1. Transport.mil users shall protect PII in accordance with (IAW) the DOD CIO PII Memorandum, dated 18 August 2006, Department of Defense (DOD) Guidance on Protecting Personally Identifiable Information (PII)). Key provisions are listed below. Ultimately, it is the responsibility of the user to ensure that PII is protected IAW with all applicable guidance:
   a. PII information with Transport.mil must be protected at a Confidentiality level of CUI.
   b. PII shall not be processed or stored on mobile computing devices or removable electronic media without expressed approval of the Authorizing Official (AO)
   c. PII stored on removable electronic media taken outside protected workplaces shall be signed in and out with a supervising official and shall be encrypted
   d. Loss or suspected loss of PII must be reported to the Functional Manager within one hour
2. Printed output products containing PII must be properly labeled. The policy for labeling output products containing Privacy Act information is DODI 5200.48 and the DOD CUI website at https://www.dodcui.mil/
3. PII must be protected from unauthorized access especially when the system is in use and when the information is printed. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a(i) provides for criminal penalties for violating PII policies.

Name (Last, First, MI)	Pers. Type (Mil/Gov/Ctr)
Directorate/Division/Branch	Work Location
DSN	E-mail
Signature	Date