

HUMAN RESOURCES COMMAND TACTICAL PERSONNEL SYSTEM TACTICAL PERSONNEL  
SYSTEM (TPS) USER AGREEMENT (UA)

For use of this form, see AR 25-2

SCOPE. This policy applies to all Soldiers, civilians, and contractors who use a Government information system (IS) that is supported and serviced by DoD authorized personnel. By signing this document, you acknowledge and consent that when you access TPS: (1) You are accessing a U.S. Government 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:

- The U.S. Government routinely intercepts and monitors communications on this IS 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 IS 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 IS includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

By signing this document, I certify that I understand the following additional requirements and I understand that this list is not all-inclusive:

- I WILL:

- Generate, store, and protect passwords/PINS IAW AR 25-2; participate in all training programs required; remove my CAC and engage the "Lock Computer" utility when away from my computer; leave my computer powered on 24 hours a day; use the "Restart" feature from the Start menu—not the "Log Off" or "Lock Computer" when leaving for the day.
- Ensure compliance with all provisions of the Data at Rest (DAR), and protection of Personally Identifiable Information (PII) policies issued by the Department of Defense and Department of the Army.
- Ensure all computers that have TPS, and all associated files loaded on them, are secured at all times, either by authorized users or being locked down when not in use.
- Be responsible for maintaining the encryption of the files and maintaining the security of the data contained on the computer at all times.
- Ensure that I have been briefed and understand my installations computer security measures and emergency response procedures if a loss of the computer or release of data should occur.

- I WILL NOT:

- Share UserID and passwords; install, connect, or use any personally owned hardware, software, or public domain software; connect any personal IT equipment (i.e. PEDs, PDAs, personal computers, USB devices, and digitally enabled devices) to my government IS or to any Government network; use unauthorized peer-to-peer software or introduce executable or malicious code; access pornography, obscene material, gambling, or gaming sites; transmit chain letters; violate/infringe copyrighted materials.

ENFORCEMENT. Any personnel violating this policy may be subject to disciplinary action under administrative, criminal, or contract-based rules, regulations, and state and federal law, and/or the Uniform Code of Military Justice (UCMJ) where applicable.

ACKNOWLEDGEMENT. I have read the above requirements regarding use/access to TPS and associated files. I understand my responsibilities regarding the protection and use of these systems and the information contained in them. I acknowledge that my signature on this document is legally binding for the duration of my employment with the DoD.

\_\_\_\_\_  
User Signature

\_\_\_\_\_  
Date