ERPIMS USER AGREEMENT

Rules of Behavior and User Agreement for Internal/External General Users

PRIVACY ACT STATEMENT

Authority: Public Law 99-474; the Computer Fraud and Abuse Act; 5 U.S.C Statute 301; 10 U.S.C. Part II; 14 U.S.C. Chapter 11; UCMJ; DOD 5500.7R, Joint Ethics Regulation; CJCSM 6510.05, Air Force Instruction 33-332, 10 March 2020.

Disclosure: Disclosure is voluntary. The personal information contained in this agreement may be used to identify you and may be disclosed to law enforcement or other authorities for investigating or prosecuting a violation of the law, regulation, policy, or this agreement. Providing the below required Privacy information by the user on this agreement is voluntary. Failure to provide the required information will result in denial of access to the Environmental Resources Program Information Management System (ERPIMS).

NAME:_____ GRADE/RANK/STATUS: _____

ORGANIZATION:_____PHONE NUMBER:_____

I. RULES OF BEHAVIOR FOR USE OF ERPIMS

- This user agreement applies to use of all ERPIMS servers, applications, and terminal equipment at the development facilities and operational locations.
- As an approved user account holder of the ERPIMS, I understand and agree that:
    - The ERPIMS capability is for official use and authorized purposes only in accordance with DoD 5500.7-R, "Joint Ethics Regulation."
    - I am responsible for ensuring that ERPIMS is used in a manner that safeguards the information contained in the system from unauthorized or inappropriate use, modification, disclosure, destruction, or denial of service
    - The U.S. Government routinely intercepts and monitors communications occurring on the government systems for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.
- ERPIMS is an unclassified mission support system designed to process data up to, but not above Sensitive "For Official Use Only."
- Remote access by the external customer (.com user community) is not supported
- You must complete all Information Assurance and Security training required by your Government organization as a prerequisite to receiving system access
- You must comply with the DoD policy regarding account management to include:
    - Account will be locked after 30 days of non-use
    - Account will be disabled after 120 days if not reactivated
    - Account will be disabled when account is no longer required. Account holder must notify ERPIMS Help Desk of changes in status (i.e. deploying , departing org, contract status change, no longer have a need-to-know).
    - Account will lockout after 3 failed login attempts and must be unlocked by an Administrator
- You must comply with the DoD policy regarding passwords, if applicable, to include:
    - Creation of strong passwords (2 upper, 2 lower, 2 special, 2 numerical; minimum 15 characters).

- Safeguarding your password (classified to the level of the network) and not share them with anyone.

- The following actions are prohibited, except as approved by the ERPIMS Configuration Control Board (CCB):
  - Connecting any Government-owned, contractor-owned, or personal hardware to the ERPIMS
  - Loading any software, shareware, or public domain software on ERPIMS
  - Upload .exe, .com, .vbs, .scr, or .bat files onto ERPIMS components
  - Changing the configuration of Government owned communications interface devices
  - Changing the configuration of ERPIMS security devices

- You are not allowed to copy, create, distribute, transmit, or retransmit any material for personal or illegal purposes.

- You are required to safeguard all printed outputs, including, but not limited to, back-up devices such as magnetic tape, disks, and removable hard drives, created, copied or stored from ERPIMS components and ensure they are marked with the appropriate classification level and data sensitivity level.

- You are not allowed to perform maintenance on any ERPIMS component without prior authorization

- You are not allowed to create or store any personal information on any ERPIMS component

- You are required to immediately report ERPIMS system or network problems, unauthorized use, and/or any actual or suspected breaches of physical, communications, operations, information or computer security to the AFCEC ERPIMS Program Manager, unit security manager and/or your Information Assurance Officer

- You are required to immediately report all suspected or known security incidents to the local security officer and/or AFCEC ERPIMS Program Manager

- You are prohibited from taking any actions that will adversely impact ERPIMS security

II.RESPONSIBILITIES ACKNOWLEDGEMENT

I have read the above rules of behavior that apply to my use of the ERPIMS. I understand my responsibilities as they pertain to using and protecting ERPIMS information. By signing this document, I acknowledge and agree to abide by the rules of behavior defined in the paragraph above.

I understand any violation of this agreement may result in disciplinary action, up to and including termination.

Signature: Date:_____