USAREC Operations Security (OPSEC) Individual User Compliance Agreement

Operations Security (OPSEC) is a key protection element that protects the Warfighter, our Anny, our families, and all the personnel that support their efforts. OPSEC relies on every individual understanding what critical information is, and knowing how to protect it. It is incumbent on every person to do their part and practice good OPSEC. Through your efforts, you can help prevent release of sensitive information that may lead to serious injury or death to personnel, damage to weapons systems, equipment, facilities, loss of sensitive technologies, and mission failure.

1. I know my critical information. Critical or sensitive information includes For Official Use Only (FOUO), information, Essential Elements of Friendly Information (EEFI) or Critical information List (CIL), Personally Identifiable I11fom1ation (PII), and information protected by the Privacy Act of 1974 as well as information covered by the Health Insurance Portability and Accountability Act (HIPAA). I have read and understand Annex. B to the TRADOC OPS EC Plan, and my unit's EEFI or CIL.

2. I know how to protect my critical information.
I will ensure waste containing critica1 or sensitive information is destroyed in a manner to prevent disclosure (e.g. shredded or burned per local policy).
I will never discard critical or sensitive infom1ation in a trash or recycle bin.
I will ensure that government conversations, web postings, blogs, social media comments, or releases to the media and/or public receive appropriate OPSEC reviews prior to being disclosed, posted or transmitted.
I will not display my security badge(s) outside secure areas. I will avoid allowing pictures to be taken of my security badge(s) and/or other sensitive information.
I will talk to my family about OPSEC and the need and obligation to protect critical information. I will not discuss or transmit sensitive information over wireless unsecure devices.
I will encrypt all e-mails that contain sensitive or critical information.
I will limit mission-related e-mail traffic to only official DoD accounts.
I will limit use of personally owned devices to only those documents that are approved for public release. I will not process DoD information on public computers (e.g., those available for use by the general public in kiosks, libraries, or hotel business centers).
When traveling, I will use encrypted connections where available (VPN, etc), and I will secure my media and documents at all times.

Acknowledgement of Responsibilities: Personnel who fail to comply with orders, directives, or policies to protect critical and sensitive information may be punished under violations of a lawful order under UCMJ, Art. 92 or under other disciplinary administrative, or other actions as applicable. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action. I acknowledge.

_____ _____
Signature Date

_____
Printed Name