

Defense Logistics Agency (DLA)

Mandatory Notice & Consent Provision for All DoD Information System User Agreements - May 9, 2008

EDA User Security and Privacy Rules of Behavior (ROB)/EDA Acceptable Use Policy (AUP) 23 May 2008

STANDARD MANDATORY NOTICE AND CONSENT PROVISION

FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

(STANDARD AGREEMENT & ANNUAL TRAINING)

By signing this document, you acknowledge and consent that when you access Department of Defense (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 (PM), law enforcement (LE), and counter-intelligence (CI) 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 the 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.

Defense Logistics Agency (DLA) Mandatory Notice/Consent/ROB/AUP

- 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.
- o 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.
- o 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.

Defense Logistics Agency (DLA) Mandatory Notice/Consent/ROB/AUP

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

All Users shall:

- Hold US Government security clearances and have completed background checks commensurate with the level of information to which they are being granted access.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Protect information and system resources against occurrences of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse or release to unauthorized persons. Immediately report all such occurrences described above to their Information Assurance Manager (IAM).
- Follow current DoD password (PW) configuration rules mandated by Joint Task Force - Global Network Operations (JTF-GNO), when a User ID and PW are required to access a system.
- Never share their passwords or PIN.
- Protect their password(s) and/or Common Access Card (CAC) personal identification number (PIN). Promptly change their password/PIN when possibly compromised, forgotten or when it appears in an audit document. Immediately notify their Terminal Area Security Officer (TASO) or their IAM if they believe their password/PIN has been compromised and promptly change their password/PIN. (Your TASO or IAM will verify that your password changed and/or PIN has been reset.)
- Ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know.
- Ensure all documents, equipment, and machine-readable media containing sensitive data are cleared, properly marked, and sanitized before being released outside of the Department of Defense. Contractors shall ensure documents, equipment, and machine-readable media containing sensitive data are cleared, properly marked, and sanitized before these items are used to support another contract. (See DoD 5200.1-R, Information Security Program for releasing documents outside of DoD.)
- Protect terminals or workstations from unauthorized access. Remove their CAC from the reader when leaving their workstation. If the workstation has not been CAC-enabled, lock it before leaving. Also, activate the desktop screen saver and set the idle time out period to 15 minutes. Contact the Service Desk for assistance in locking the workstation and activating the screen saver.
- Ensure that devices that display or output sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information and/or obtain a Privacy screen filter for your monitor.
- Inform the supervisor when access to a particular DoD information system or enclave is no longer required (e.g., completion of project, transfer, retirement, and resignation).
- Observe rules and regulations governing the secure operation and authorized use of a DoD information system or enclave; Use the DoD information system or enclave only for authorized purposes; Not introduce malicious code into any DoD information system or enclave or physically damage the system or enclave.

Defense Logistics Agency (DLA)
Mandatory Notice/Consent/ROB/AUP

- Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed; users shall coordinate the procedure with the IAM and receive written approval.
- Not introduce or use unauthorized software, firmware, or hardware onto the DoD information system or enclave.
- Not relocate or change DoD information system or enclave equipment or the network connectivity of equipment without proper IA authorization.
- Not use wireless enabled equipment while physically connected to the system
- Understand that system use constitutes consent to monitoring, recording and auditing.

Additionally, Administrative and Privileged users shall:

- Utilize public key (PK)-enabled government owned or controlled computers that have wireless computing capabilities disabled.
- Connect to the system using FIPS 140-2 validated virtual private network (VPN) software when authorized to work remotely.
- Follow current DoD password (PW) configuration rules mandated by Joint Task Force - Global Network Operations (JTF-GNO), when a User ID and PW are required to access a system.

Exceptions granted by an Information Assurance Officer or an Information Assurance Manager to any of the above rules shall be confirmed in writing and provided to the Deputy Designated Accrediting Authority (DAA) for the Defense Logistics Agency.

If you have any questions or comments about the information presented here, please contact the Service Desk.

Defense Logistics Agency (DLA) Mandatory Notice/Consent/ROB/AUP

Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Annual User Training

- You may be granted access to personal information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., social security number, age, rank/grade, marital status, race, salary, medical information or complete personal bank account number, etc. Such information is also known as personally identifiable information (PII).
- The computer screen where personally identifiable information appears must be labeled with "For Official Use Only" Privacy Act of 1974, As amended." If the system cannot be changed to have this appear on each screen, it must be on the log-in screen to the system, or a Privacy label may be placed on the computer monitor. The Privacy label shall read, "Personal Data Privacy Act of 1974, as Amended, 5 U.S.C. 522a.
- Printed output products must be properly labeled with "For Official Use Only" "Privacy Act of 1974, As amended." The policy for labeling output products containing Privacy Act information is in DoD 5200.1-R, Appendix 3, page 141 and DoD 5400.11-R, paragraph C1.4.
- Place the standard Privacy Act warning label on the top of your computer monitor if names and social security numbers/personal bank account numbers, etc., are on your computer screen while you do your work. These labels can be generated on a plain white label that must read: "Personal Data, Privacy Act of 1974, as Amended, 5 U.S.C. 522a."
- PII in DoD systems 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) also provides for criminal penalties.
 - (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain personally identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.
 - (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)
 - (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.
 - (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.
- If you have any questions or comments about the information presented here, please contact the Service Desk.

**Defense Logistics Agency (DLA)
Mandatory Notice/Consent/ROB/AUP**

User's Acknowledgement of Mandatory Agreement, Security and Privacy Training

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- I have read and consent to the terms in the Standard Mandatory Notice & Consent Provision for All DOD Information System User Agreements (Standard Agreement Training).
- I have read and consent to the terms in the System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.
- I have read and consent to the terms in the Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.
- I also agree to follow the standard agreement and these rules as a condition of being granted system access.

(Print your DoD Component/office and indicate you have read each section. Then print your full name, sign and date this document.)

DoD Component/Office _____

---- Check box if you have read this agreement

I have read the Mandatory Agreement & Consent Training	Yes
I have read the System Security ROB/AUP Training	Yes
I have read the Privacy ROB/AUP Training	Yes

Print Full Name (Last, First, Middle) _____

Signature _____ **Date** _____

----- Attach this completed signature page to the DD Form 2875 at the time submission. -----