PRIVILEGED ACCESS AGREEMENT (PAA) &
ACKNOWLEDGEMENT OF RESPONSIBILITIES

Submit by Email

Print Form

organization

I understand that I have access to ☐ NIPR ☐ SIPR ☐ JWICS ☐ NSA ☐ SAP ☐ TS Army IS, and that I have and will maintain the necessary clearances and authorizations for privileged access to System

As a privileged-Level user;

I will protect the **root, administrator,** or **superuser** account(s) and authenticator(s) to the highest level of data or resource it secures.

I will **NOT** share the **root, administrator,** or **superuser** account(s) and authenticator(s) entrusted for my use.

I am responsible for all actions taken under my account and understand that the exploitation of this account would have catastrophic effects to all networks for which I have access. I will ONLY use the special access or privileges granted to me to perform authorized tasks or mission related functions.

I will only use my privileged account for official administrative actions.

I will not attempt to "hack" the network or connected ISs, subvert data protection schemes, gain, access, share, or elevate permissions to data or ISs for which I am not authorized.

I will protect and label all output generated under my account to include printed materials, magnetic tapes, external media, system disks, and downloaded files.

I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of system or network services, illegal or improper possession of content or files, or the
actual or possible compromise of data, files, access controls, or systems to the Information Assurance Office.

I will NOT install, modify, or remove any hardware or software (i.e. freeware/shareware, security tools, etc.) without permission and approval from the Information Assurance Office.

I will not install unauthorized or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc) or hardware.

I am prohibited from obtaining, installing, copying, pasting, modifying, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, or license agreements.

I will not create or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS or networks under my privileged account.

I am prohibited from casual or unofficial web browsing and use of email while using the privileged-level account. This account will NOT be used for day-to-day network communications.

I am prohibited from accessing, storing, processing, displaying, distributing, transmitting and viewing material that is; pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, national, or international law.

I am prohibited from storing, accessing, processing, sharing, removing, or distributing Classified, Proprietary, Sensitive, Privacy Act, and other protected or privileged information that violates established security and information release policies.

I am prohibited from promoting partisan political activity, disseminating religious materials outside an established command religious program, and distributing fund raising information on activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g. command social-event fund raisers, charitable fund raisers, etc).

I am prohibited from using, or allowing others to use, Army resources for personal use or gain such as posting, editing, or maintaining personal or unofficial home pages, web-blogs, or blogging sites, advertising or solicitation of services or sale of personal property (e.g. eBay) or stock trading.

I am prohibited from employing, using, or distributing personal encryption capabilities for official electronic communications. I will contact the Information Assurance Office if I am in doubt as to any of my roles, responsibilities, or authorities.

I understand that all information processed on ISs is subject to monitoring. This includes E-mail and Web Browsing.

I will obtain and maintain required certification(s) in accordance with DoD and Army policy to retain privileged level access.

PRIVILEGED ACCESS AGREEMENT (PAA) &
ACKNOWLEDGEMENT OF RESPONSIBILITIES

I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged access roles and may result in any of the following actions:

a. Chain of command revoking IS privileged access and/or user privileges
b. Counseling
c. Adverse actions under the UCMJ and/or criminal prosecution
d. Discharge or Loss of Employment
e. Revocation of Security Clearance

Requestor is required to upload approved PAA to their ATCTS profile.

Date: _____ User Signature: _____

This portion must be signed and approved by the Information Assurance Manager after all prerequisites have been validated.

☐ Annual IA Awareness Training

☐ ATCTS Registration

☐ Appropriate IA Duty Appointment letter and Acceptable Use Policy (AUP) have been uploaded to ATCTS

Date: _____ IAM (I/II) Signature: _____

CERTIFICATE OF NON-DISCLOSURE

Disclosure of protected or privileged information

Whoever, being an officer, employee or agent of the United States or of any department, agency or contractor thereof, publishes, divulges, discloses or makes known in any manner or to any extent not authorized by law, any information coming to him/her in the course of their employment or official duties, which information concerns or relates to the trade secrets or proprietary information of a non-Federal government entity; any information protected by the Privacy Act; any information subject to protection under the Freedom of Information Act; other law, regulation, or policy (including all privileged communications such as doctor-patient, attorney-client, etc.); any information protected under the classification system set forth in AR 380-5; or any other information protected by law or regulation (i.e. IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to UCMJ, administrative, or contract remedy enforcement.

CERTIFICATION

I have read the provisions herein and I understand my responsibility not to disclose any matters connected with or pertaining to these provisions as they pertain to my organization's network except to persons theretofore listed as having a need to know.

Date: _____ User Signature: _____