FORT KNOX PRIVILEGED-LEVEL ACCESS AGREEMENT (PAA)

For use of this form, see Army Regulation (AR) 25-2; Best Business Practice (BBP) 06-PR-M-0003;
and RMF Controls AC-2, AC-2(7), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AT-3, PS-4, PS-5, AT-3, MP-3, PS-6, RA-5, and SI-2.

Name: _____ EDIPI: _____

Organization: _____ Enterprise Email Address: _____

SECTION I – ACKNOWLEDGEMENT OF RESPONSIBILITIES

I understand that I have privileged-level access to the selected network enclave(s) below, and that I will maintain the necessary clearances, certification/training, and any additional authorizations required. I understand that I am required to upload my signed and approved PAA to my Army Training and Certification Tracking System (ATCTS) profile.

☐ NIPR (NASE) ☐ SIPR (CONUS) ☐ RSN ☐ HRC

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 information systems (ISs), subvert data protection schemes, gain, access, share, and/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 my supporting Information Systems Security manager (ISSM).
- I will NOT install, modify, and/or remove any hardware and/or software (i.e. freeware/shareware, security tools, etc.) without permission and approval from my supporting ISSM.
- I will not install unauthorized and/or malicious code, backdoors, software (e.g. games, entertainment software, instant messaging, collaborative applications, etc.) and/or hardware.
- I am prohibited from obtaining, installing, copying, pasting, modifying, transferring and/or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade-secret, and/or license agreements.
- I will not create and/or elevate access rights of others; share permissions to ISs for which they are not authorized; nor allow others access to IS and/or networks under my privileged-level 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/or viewing material that is pornographic, racist, defamatory, vulgar, hate-crime related, subversive in nature, and/or involves chain letters, spam, or similarly related criminal offenses such as encouragement of criminal activity, or violation of State, Federal, National, and/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 my ISSM 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 email and web browsing.
- I will obtain and maintain required Baseline certification(s) and Computing Environment (CE) certifications/training in accordance with Department of Defense (DoD) and/or Army policy to retain privileged-level access.
- I will use and protect the Alternate Smart Card Logon (ASCL) token issued to me. I also understand that I am responsible for turning in the token when I leave the position for which the token was issued.

- I will maintain Information Assurance Vulnerability Management (IAVM) compliance, and subscribe to the IAVM notice email alerts.
- I understand that this form will expire when one of the following exist: A Change of Command or the expiration of my current ASCL token.
- I understand that failure to comply with the above requirements is a violation of the trust extended to me for the privileged-level access roles, and may result in any of the following actions:
  a. Chain of command revoking IS privileged-level access and/or user privileges.
  b. Counseling.
  c. Adverse actions under the Uniform Code of Military Justice (UCMJ) and/or criminal prosecution.
  d. Discharge or loss of employment.
  e. Revocation of security clearance.

Certificate of Nondisclosure 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 his/her employment or official duties, of which any of the information concerns or relates to the trade secrets or propriety 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 (IG, AAA, CID); shall, in addition to any penalty imposed by said law or regulation, be subject to the Uniform Code of Military Justice, administrative, or contract remedy enforcement.

My digital signature below indicates that I have read the PAA and Certificate of Nondisclosure of Protected or Privileged Information in Section I herein, and I understand it is my responsibility to abide by these provisions as they pertain to my Organization's network.

Date: _____ User's Signature: _____

SECTION II – CERTIFICATION

This form must be resigned by all parties upon renewal of ASCL token and/or when there is a change in signatory.

This portion must be signed and approved by the NASE Information Systems Security Manager (ISSM) for access to NASE elevated privileges.

☐ ATCTS Registration ☐ Annual IA Awareness Training ☐ Cyber Security Fundamentals within last 24-months

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

Date: _____ NASE ISSM Name: _____ NASE ISSM Signature: _____

This portion must be signed and approved by the CONUS ISSM for access to CONUS elevated privileges.

☐ ATCTS Registration ☐ Annual IA Awareness Training ☐ Cyber Security Fundamentals within last 24-months

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

Date: _____ CONUS ISSM Name: _____ CONUS ISSM Signature: _____

This portion must be signed and approved by the RSN ISSM for access to RSN elevated privileges.

☐ ATCTS Registration ☐ Annual IA Awareness Training

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

Date: _____ RSN ISSM Name: _____ RSN ISSM Signature: _____

This portion must be signed and approved by the HRC ISSM for access to HRC elevated privileges.

☐ ATCTS Registration ☐ Annual IA Awareness Training

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

Date: _____ HRC ISSM Name: _____ HRC ISSM Signature: _____