# INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGMENT OF RESPONSIBILITIES

Date:

1. I understand there are DoD Information Systems (IS), classified and unclassified, and that I have the necessary clearance for privileged access to
I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.

2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the
As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers who are not authorized access.

3. I understand that I am responsible for all actions taken under my account(s), root, or otherwise. I will not attempt to "hack" the network or any connected information systems, or gain access to data to which I do not have authorized access.

4. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).

5. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate
Information Assurance Management (IAM) or Wing Information Assurance Office(WIAO). I will NOT install, modify, or remove any hardware or software (i.e. *e.g.*, freeware/shareware and security tools) without written permission and approval from the Information Assurance Manager (IAM) or Wing Information Assurance Office(WIAO).

6. I will not install any *unauthorized* software (e.g., games, entertainment software) or hardware (e.g., sniffers).

7. I will not add/remove any users' names to the Domain Administrators, Local Administrator, or Power Users group without the prior approval and direction of the
IAM/or WIAO.

8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the local area networks.

9. I understand that I am prohibited from the following while using the DoD IS:

a. Introducing Classified and/or Controlled Unclassified Information (CUI) into a NIPRNet environment.

b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.

c. Storing, accessing, processing, or distributing Classified, Proprietary, CUI, For Official Use Only (FOUO), or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

f. Engaging in prohibited political activity.

g. Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker).

h. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers and charitable fund raisers, without approval).

i. Gambling, wagering, or placing of any bets.

j. Writing, forwarding, or participating in chain letters.

k. Posting personal home pages.

l. Any other actions prohibited by DoD 5500.7-R (Reference (y)) or any other DoD issuances.

10. Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

11. I understand that if I am in doubt as to any of my roles or responsibilities I will contact Information Assurance Manager (IAM) or Wing Information Assurance Office for clarification.

12. I understand that all information processed on the
is subject to monitoring. This includes email and browsing the web.

13. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from the
IAM.

14. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission related functions.

15. I will not use any DOD/Air Force owned information system to violate software copyright by making illegal copies of software.

16. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day to day network communications.

17. I understand that failure to comply with the above requirements will be reported and may result in the following actions:

a. Revocation of IS privileged access.
b. Counseling.
c. Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution.
d. Disciplinary action, discharge or loss of employment.
e. Revocation of Security Clearance.

18. I will obtain and maintain required certification(s), according to DoD 8570.01-M and the certification provider, to retain privileged system access.

IAT (User) Name: Date:

IAT (User) Signature:

System IAO or Unit ORG IAO Name: Date:

System IAO or Unit ORG IAO Signature: