Enclosure D

Fleet and Family Readiness NAF Enterprise Network Privileged User Agreement

INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

1. I understand there are two DoD Information Systems (IS), classified (SIPRNet) and unclassified (NIPRNet). I understand that the Navy Fleet and Family Readiness (FFR) Non-Appropriated Fund (NAF) Enterprise Network is an unclassified, private, commercial network operating the systems of the FFR Accounting and Information Management System (AIMS), and that I have the necessary clearance for privileged access to the FFR NAF Network. I will not introduce or process data for the Information System (IS) which 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 FFR NAF Network. 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 FFR NAF Network privileged access.

3. I understand that passwords for all accounts with elevated privileges (Service Accounts, System Administrators, Backup Operators, etc.) must comply with Department of Defense requirements for privileged user password complexity. Personnel with elevated privileges will comply with FFR NAF Network two-factor authentication requirements for remote network access.

4. I understand that I am responsible for all actions taken under my account(s). I will not attempt to gain access to data, FFR NAF Network devices, systems, or any interconnected systems to which I do not have authorized access.

5. 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).

6. 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 FFR NAF Network Information Assurance (IA) personnel, security personnel, or senior management. I will not install, modify, or remove any hardware or software without written permission and approval from FFR NAF Network IA (N946) or the FFR NAF Network Configuration Control Board.

7. I will not install any unauthorized software (e.g., games, entertainment software, etc) or hardware (e.g., sniffers).
8. I will not add any users’ names to the Domain Admins, Local Administrator, or Power Users group without the prior approval and direction of FFR NAF Network IA or the Configuration Control Board.

9. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the FFR NAF Network wide or local area networks.

10. I understand that I am prohibited from the following while browsing the web:
    a. Introducing Classified and/or Unclassified Controlled Information (UCI) into an unclassified system or 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, UCI, 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. Promoting partisan political activity.
    g. Disseminating materials unrelated to an established command religious program.
    h. 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).
    i. Fundraising 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., without approval).
    j. Gambling, wagering, or placing of any bets.
    k. Writing, forwarding, or participating in chain letters.
    l. Posting personal home pages.

11. I understand that personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.
12. I understand that if I am in doubt as to any of my roles or responsibilities I will contact FFR NAF Network management personnel for clarification.

13. I understand that all information processed on the FFR NAF Network is subject to monitoring. This includes e-mail and browsing the web. I will not attempt to circumvent any monitoring, auditing or logging mechanisms deployed on the FFR NAF network.

14. 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 FFR NAF Network IA Management.

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

16. I will not use any FFR owned information systems to violate software copyright by making illegal copies of software.

17. I will use my PRIVILEGED USER account only for official administrative actions. I will not use my account for day-to-day network communications.

18. I understand that failure to comply with the above requirements will be reported and may lead to the following actions:
   a. Chain of command revocation of FFR NAF Network privileged access and/or user privileges
   b. Counseling
   c. Adverse actions under the Uniform Code of Military Justice and/or criminal prosecution
   d. Disciplinary action, discharge or loss of employment

19. I will obtain and maintain required certification(s), competency, and training to retain privileged system access.

USER NAME______________________________________

SIGNATURE___________________________________________________

DATE_______________________________________

FACILITY______________________________________

INFORMATION SYSTEM: FFR NAF Enterprise Network