Application for User Access to Office of Naval Research SIPRNET

USER INFORMATION

1. Full Name _____

2. User Contract Email (userid@onr.navy.mil): _____

3. Select one ☐ Contractor ☐ Government ☐ Reservist ☐ Detailee ☐ Military ☐ IPA

4. Code Number: _____ 5.User Phone Number: _____

6. Contract Number: _____ 7.User Room Number: _____

8. If contractor, Company Name: _____

9. Comments: _____

10. I have read, understand, and agree to comply with all of the Information Security and Network Security issues and requirements associated with access to the ONR Siprnet. I have read and will abide by the security safeguards listed in the document Security Operating Procedures. I have a need to know, am a US Citizen, and I posses a current security clearance at the proper level (SECRET or higher) to access the Siprnet.

11. Applicant Signature: _____ 12. Date: _____

Administrative Officer (AO)

13. AO Name: _____ 14. AO Code: _____

15. AO Email Address: _____

16. Clearance Information (ONR Security Office)

ONR Security Office One Liberty Center (OLC) 6th Floor Room 624, Phone (703) 696-6845

a. Clearance Verification:

(1) Verifying Officer Name: _____

(2) Verifying Officer Signature: _____

(3) Access Level: _____

b. Applicant Security Clearance Information

(1) Date Granted: _____

(2) Granted By: _____

(3) Badge Expiration Date: _____

c. As the Administrative Officer of the above named employee, I certify that he/she:

has the need to know classified information described above, and
has a current Security Clearance at the appropriate clearance level (SECRET or higher)

Applicant Signature: _____ Date: _____

Please FAX completed application to ONR Helpdesk (703) 696-6156, Please print clearly.
All SIPRNET email accounts will be available within 3 days.
For questions or status information, email helpdesk@onr.navy.mil.

SIPRNET USER ACKNOWLEDGEMENT

As a user of the Secret Internet Protocol Router Network (SIPRNET), I acknowledge my responsibility to conform to the following requirements and conditions. These requirements and conditions are established for and apply to all AISs (Automated Information Systems) connected to the SIPRNET.

1. I understand that failure to sign this acknowledgment will result in denial of access to the SIPRNET.

2. I understand that the network operates in the SECRET System High mode and I assert that I have all clearances necessary for access to the network. I will NOT introduce or process data which the network is not specifically authorized to handle. Specifically, the SIPRNET is authorized to contain, handle, and process all Information up to and including collateral SECRET U. S. ONLY. Any information classified as TOP SECRET (with or without categories and /or caveats) with any categories and/or caveats will NOT be allowed on the SIPRNET domain.

3. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account.

4. I understand that I am responsible for all actions taken under my account. I will NOT attempt to "hack" the network or any connected MS or network or attempts to gain access to data for which I am not specifically authorized or to exceed my authorization.

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

6. I understand my responsibility to report and/all AIS or network problems to the AIS/network administrator. I will NOT install/modify/remove any hardware or software without the permission of the AIS/network administrator.

7. I acknowledge my responsibility to use the network ONLY for official government business.

8. I acknowledge my responsibility NOT to introduce any software or hardware not acquired through official channels. I also acknowledge my responsibility to virus-scan all official software before introducing it into the AIS or network.

9. NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINSTUNATHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION UNDER TITLE 18 U.S.CODE. EVIDENCE OF UNATHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

10. I acknowledge my responsibility to conform to these requirements and conditions when using the SIPRNET. I also acknowledge that failure to comply with the requirements and conditions may constitute a security violation and/or a violation of either Agency policy or regulation resulting in denial of access to the SIPRNET. Additionally, such violations will be reported to the appropriate authorities for further action as deemed appropriate.

Signature: _____ Date: _____