NETWORK SERVICES ACCOUNT REQUEST

(Please Complete this form and return to the HELP DESK)

1. Rec'd by:

Date: _____

Time: _____

2. Kind of Request

☐ New Account ☐ Delete Account ☐ Change Account ☐ Check-out

3. Effective Date:

4. Account Type

☐ PC ☐ E-Mail ☐ INRIS ☐ CAMIS ☐ SIPRNET ☐ Secure PC ☐ Hopper

5. User Information:

☐ MS. ☐ MRS. ☐ MR. ☐ DR. ☐ Rank _____	**a. NAME: Last**	**First:**	**Middle Initial:**
	b. Code:	**c. Phone:**	**d. Bldg / Rm No.:**

e. Status:

☐ ONR / Govt ☐ Detailee ☐ Contractor Company _____ ☐ Reservist Unit _____ ☐ Military ☐ Temp

f. Previous ONR Account: ☐ YES ☐ NO

6. Shared/Group Directories Access:
If not known, list like "User....."

7. E-Mail Distribution List Membership:
If not known, list like "User....."

8. If this a DELETE ACCOUNT REQUEST, please indicate what is to be done with the Client's Files:

9. NOTES / SPECIAL INSTRUCTIONS:

10. AO Signature (Required): _____

INRIS Account Information

MUST BE APPROVED BY KEY USER

☐ New Account ☐ Expire Account ☐ Delete Account

Key User Signature: _____ **Initials**

Will Need Access to the Following:
(Please check one)

Menu Role: _____ _____

☐ Acquisition
☐ Finance
☐ Science & Technology
☐ Corporate
☐ Other (specify)

Job Assignment _____ _____

User ID _____ _____

Oracle ID _____ _____

Personnel Data _____ _____

ONR-HQ network and Secure-PC

Security Awareness Briefing

The importance of information Systems Security (INFOSEC)

1. The ONR-HQ Network and INRIS are designated Sensitive Unclassified systems
2. Under applicable Federal, DCD, and DON regulations - Protection is required by Public Law 100-235 Computer Security Act of 1987.
3. Sensitive data must be protected from unauthorized use or disclosure.
4. Financial Data, Privacy Act Data and Contractual Data are all maintained in INRIS.

Password Policy

1. Passwords should be at least 6 characters and at least 1 numeric character
2. Passwords will expires every 180 days.
3. To prevent users from changing their new password right back to their old password, the minimum age of new passwords is 5 days.

Screen Saver Time Out

1. Password protected screen savers protect access to your workstation during long periods of absence from your desk.

Computer Viruses

1. Do NOT download files off the Internet to LAN drives.
2. Do NOT download files off the Internet to your hard drive.
3. Download files off the Internet to a floppy diskette only.
4. Virus checkers are loaded on all ONR-HQ LAN workstations. Do NOT disable them.
5. Be careful of the diskettes you bring into the office.
6. Call the helpdesk when you suspect your workstation has been infected.

Virus Hoaxes

1. Be aware that virus hoaxes exist.
2. Do not forward any virus warnings on the ONR Network to anyone other than the ISSM. The ISSM will determine if the warning is authentic or a hoax.

Critical Information

1. Critical information with which you choose to save to your workstation's hard drive, should also be backed-up to a floppy disk.
2. You may also save critical information to a network drive. All network drives are backed-up daily.

Classified Material

1. NO classified material shall ever be put on the ONR-HQ Network.
2. The SECURE-PC, a stand-alone computer system approved to process classified information is available to people working at ONR who have a security clearance. It is located in room 528-2 for classified computing needs.

Log-off

1. At the end of the workday you must logoff the ONR-HQ Network account and power off the workstation.
2. You must also log-off when completing use of the SECURE-PC, power off the workstation and return the removable hard disk to the proper custodian for safekeeping.

ONR has invested significant resources in the ONR Network and INRIS. These systems are critical to ONR's mission and day to day operations. Your participation in protecting the systems is appreciated and required.

You may call Vera Jones at 696-0708 with questions regarding INFOSEC.