

LAN ACCOUNT REQUEST FORM

First Name _____ MI _____ Last Name (PRINT CLEARLY) _____

Rank/Rate/Grade _____

Work Address (Street Address) _____

City _____ State _____ ZIP _____

Company / Activity and Base _____

Work Phone _____ Office (Building / Room #) _____

PRD _____ Security Clearance _____

If known, to which E-Mail distribution lists should you be added?

1. _____ 2. _____

If known, to which LAN folders do you need access?

1. _____ 2. _____

Supervisor Name _____

Supervisor Signature _____ Date _____

CSSC/STOREFRONT USE ONLY

Original Statement of Use Form on File (Location and Technician Initials) _____

Account Creation Date _____ User Name _____

Connection Type(s): Dial-Up _____ Direct _____

Domain Name _____

E-mail Alias Server Assigned _____

Display Name _____

Groups Assigned _____

Server and Home Directory Path _____

Account Created By (Technician Name) _____

LAN Account Deletion Date _____

Account Deleted By (Technician Name) _____

COMMANDER, NAVY REGION
MID-ATLANTIC
PROGRAM MANAGER FOR
INFORMATION TECHNOLOGY

Customer Service Support Center

LAN Account Request Form



Tel: 757 444-HELP

Steps to Obtain and Keep a LAN Account:

1. Complete both sides of the LAN Account Request Form and have your supervisor sign your request. Enter "N/A" in any block that would contain a blank. Ensure that you sign and date the Statement of Use form at right.
2. Detach the form from this portion and fax both sides of the completed form to NABLC ITSF at (757) 462-3143.
3. CSSC will notify you and assist you through your initial login when access has been granted by the appropriate servicing storefront activity.
4. You will be notified by E-mail from the appropriate servicing Information Systems Security Officer (ISSO) from your activity requiring you to complete a short Computer Based Training (CBT). This CBT must be completed and verified by your supervisor within 30 days of your initial LAN access.
5. The E-mail you receive from the ISSO will have a form attached that must be filled out and faxed back to the number listed in the E-mail you received notifying you of the CBT requirement.
6. Failure to complete steps 4 or 5 will result in revocation of your access privileges.
7. You will create your own password in accordance with the requirements set forth in the Statement of Use.
8. If your account is not accessed for 90 days, your access will be suspended. If no request for reinstatement is received within 90 days from that point (180 days from last login), your account will be deleted from the system.
9. Your computer is preloaded with command approved software. Introduction of any software or upgrade without the express approval of the servicing storefront is prohibited. Attempted installation without approval could result in revocation of access privileges.
10. Special access requirements, such as dial-up access while traveling, are handled on a case-by-case basis. Please contact CSSC for assistance with your special requirement.

Tear off and save this portion for reference.

STATEMENT OF USE

Warning: this account will provide full and unlimited access to the Internet. All personnel are encouraged to use their government computers as the preferred and routine choice to access, develop, and exchange information and to develop their information technology skills. Any permissible use of the Internet enhances the users' professional skills and thus serves a legitimate public interest. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction, or command policy. Prohibited uses include:

- Introducing classified information into an unclassified system or environment
- Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature
- Accessing, storing, processing, or distributing classified, proprietary, sensitive, FOUO, or privacy act protected information in violation of established security and information release policies
- 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
- Obtaining, installing, copying, pasting, transferring, or using software obtained through other than official means
- Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses
- Promoting partisan political activity
- Disseminating religious materials outside an established command religious program
- Using the system for personal financial gain
- Fund-raising activities, either for profit or non-profit, unless specifically approved by the command
- Gambling, wagering, or placing of any bets
- Writing, forwarding, or participating in chain letters
- Posting personal home pages
- Participating in worldwide chat rooms
- Subscribing to mailing lists and Instant Messenger

NOTICE

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 against unauthorized 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. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

PASSWORDS

You will create your own individual password consisting of 8 Alpha-Numeric characters, with at least one Capital Letter and one number. Your password is never to be shared with anyone else. You will be required to change your password every 90 days.

STATEMENT OF CONSENT

By my signature below, I certify that I understand and will comply with staff security policies and procedures, I consent to periodic Information System Security audits by the COMNAVREGMIDLANT Information System Security Manager or a designated representative in compliance with all information system security rules and regulations. I understand that I must take the Information Assurance Training within 30 days or my LAN account will be terminated.

User Signature

Date