

SIPRNET LAN ACCOUNT REQUEST

Last Name, First Name MI

Rank/Rate/Grade

Command Short Name & Office Code

Work Address (Street Address)

City State ZIP

Command Long Name/ and Base

Work Phone Office (Building / Room #)

Security Clearance

Supervisor Name (printed)

I certify that the person applying for this SIPRNET ACCOUNT has a valid need for the account and has the proper clearance(as sited above). I have obtained a Visit Request for this person and will provide the Original to the Servicing Storefront Manager.

Supervisor Signature Date

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

Account Creation Date User Name
Connection Type(s): Dial-Up Direct

Dial-Up Direct
OCEANA/STOREFRONT USE ONLY

CNRMA.NAVY.SMIL.MIL
Original Domain Name

E-mail Alias Server Assigned

Display Name

Groups Assigned

Account Created By (Technician Name)

Visit Request Expiration Date (also SIPRNET ACCT EXPIRES)

Account Deleted By (Technician Name)

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

**SIPRNET LAN Account
Request Form**



Tel: 757 433-2531

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, transfer-ring, or using software or other materials obtained in violation of the appropriate vendor's patent, copy-right, trade secret, or license agreement
- Obtaining, installing, copying, pasting, transfer-ring, 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

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.

Password

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

