

New Mexico Army National Guard Network

COMPUTER-USER AGREEMENT/ NEW USER REQUEST

Your system administrator (SA) or information assurance security officer (IASO) will ask you to sign a copy of this agreement before issuing you a network username and password.

As a user of an information system, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
2. I will not import any Government-owned software or install hardware on any Government computer (GC) (for example, client-workstation, server) without first getting written approval from my commander, SA, or IASO.
3. I will not load any software onto my GC, Government information technology (IT) system, or network without the approval of my commander, SA or IASO.
4. I will not try to access data or use operating systems or programs, except as specifically authorized.
5. I know I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them—
 - a. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report to my SA for a new one.
 - b. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.
 - c. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.
 - d. If I have a classified account, I will ensure that my password is changed at least once every 90 days or if compromised, whichever is sooner.
 - e. If I have an unclassified account, I will ensure that my password is changed at least twice a year or if compromised, whichever is sooner.
 - f. I understand that if my password does not meet current DOD standards, I am to inform my SA.
 - g. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media unless approved in writing by the IASO.
 - h. I will not tamper with my GC to avoid adhering to DOD password policy.

- i. I will never leave my classified GC unattended while I am logged on unless the GC is protected by a “password protected” screensaver.
6. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.
7. I know that if connected to the Secret Internet Protocol Router Network (SIPRNET), my system operates at least in the U.S. Secret, “system-high” mode.
 - a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process). In other words, any disk going into a Secret system is now Secret and must be handled accordingly.
 - b. I must protect all material printed out from the SIPRNET at the system-high level until I or someone with the appropriate clearance personally reviews and properly classifies the material.
 - c. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the IASO.
 - d. If connected to the SIPRNET, only U.S. personnel with a security clearance are allowed unescorted access to the system.
 - e. Magnetic disks or compact disks will not be removed from the computer area without the approval of the local commander or head of the organization.
8. My local IASO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the SA or IASO.
9. I will scan all magnetic media (for example, disks, CDs, tapes) for malicious software (for example, viruses, worms) before using it on a GC, IT system, or network.
10. I will not “air gap” information using magnetic media from a classified system to an unclassified one.
11. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO and delete the message.
12. I will not run “sniffer” or any hacker-related software on my GC, Government IT system, or network.
13. I will not download file-sharing software (including MP3 music and video files) or games onto my GC, Government IT system, or network.
14. I will not connect any personal IT equipment (for example, PEDs and PDAs (such as Palm Pilots), personal computers, digitally enabled devices) to my GC or to

any Government network without the written approval of my commander, SA, or IASO and IMO.

15. I will ensure that my anti-virus software on my GC is updated at least weekly.
16. I will not use Internet "chat" services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my AKO account.
17. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.
18. I will comply with security guidance issued by my SA and IASO.
19. If I have a public key infrastructure (PKI) certificate installed on my computer (for example, software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.
20. I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.
21. I know I am subject to disciplinary action if I violate DOD computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.

AKO USER NAME:

New user Signature: _____

Date: (MM/DD/YYYY)

IASM NAME:

IASM Sig: _____

Date: (MM/DD/YYYY)

IDT SOLDIER [] (If checked no email account will be created)

Supervisors email address:

Supervisors Signature: _____

Date Requested: (MM/DD/YYYY)
