

ACCEPTABLE USE POLICY (AUP) FOR THE NORTH CAROLINA NATIONAL GUARD

- 1) **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the NGNC Enterprise Network and by extension, the Department of Defense (DOD) Non-classified Internet Protocol Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET) from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use in accordance with AR 25-2.
- 2) **Access.** Access to these networks or this system is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.
- 3) **Scope:** The scope of this agreement includes compliance to DoD and Army regulatory guidance as it applies to both wired and wireless technologies. Wireless technologies include mobile computing devices (MCD) such as laptops, handhelds, personal digital assistants (PDAs) whether operating in either wired or wireless modes, or other wireless information technologies as they are developed and fielded for processing, transmitting, or connecting locally and / or remotely to DoD information or enclave resources. The remote user will adhere to DoD policy in regard to facility clearances, protection, storage, etc. Specific items related to wireless are as follows:
 - a) All wireless systems must have Designated Approving Authority (DAA) approval.
 - b) Ensure personally owned Personal Electronic Devices (PED) are not used to transmit, receive, store, or process DoD information.
 - c) Wireless devices are often portable and must be physically protected at all times.
 - d) Ensure wireless devices are not operating in areas where classified information is electronically stored, processed, discussed or transmitted.
 - e) Ensure Bluetooth devices are not used to store, process, or transmit DoD information, unless FIPS 140-2 compliant devices are used to encrypt the data during transmission.
 - f) Do not use Bluetooth devices for classified data.
 - g) Ensure antivirus software and data at rest is properly configured for all wireless clients.
 - h) Do not use Wireless Wide Area Network systems for classified processing.
 - i) RFID systems must comply with DoD security requirements.
 - j) Infrared (IR) keyboards and mice are not authorized for use.
 - k) PDA and SMARTPHONES must display the DoD logon banner
 - l) Do not discuss classified / sensitive information on unclassified cell phones
 - m) Devices, such as PDAs and SMARTPHONES with digital cameras (still and video), are not allowed in areas processing or storing classified material.
 - n) Ensure PDAs are not used to transmit, receive, store, or process classified data.
 - o) PDAs will not be connected via hot-sync or ActiveSync to a classified workstation.
 - p) Ensure PDAs and SMARTPHONES are protected by authenticated login procedures to unlock the device. Either CAC or PIN authentication is required.
 - q) Ensure FIPS 140-2 certified encryption tools are used to encrypt unclassified data at rest on the wireless device.
 - r) Ensure mobile code is not downloaded from non-DoD sources and is downloaded from only trusted DoD sources over assured channels.
 - s) Ensure wireless radios / IR ports on PDAs / SMARTPHONES are disabled when wireless / IR transmissions are not being used. Limit use to trusted DoD devices.
 - t) PDAs with text messaging cannot be used for sensitive data.
- 4) **Revocability.** Access to Army resources is a revocable privilege and subject to content monitoring and security testing.
 - a) NGNC Information Assurance (IA) and IA support personnel may suspend access privileges if they believe it necessary to maintain the integrity of computer systems or networks. If legal violations, security threats, or violations of NGNC policies are suspected, system managers should also inform appropriate authorities. At a minimum, Information Assurance Personnel will be notified.
 - b) Installation of any software not already approved for use must be authorized by the NGNC IA Manager. Any individual that downloads and / or installs unauthorized peer-to-peer (P2P) software (including but not limited to Bittorent, Lime Wire, Kazaa, and Skype) onto a government system will have their network accounts disabled and (upon each offense) will require counseling from their O-6 or equivalent in their chain of command to have their accounts restored.
 - c) Failure to follow any of the above procedures, the signed AUP, proper security policies and regulations will result in immediate suspension of network access and privileges until compliance is confirmed by the NGNC Information Assurance Branch.

- 5) **Standard Mandatory Notice and Consent Provision.** By signing this document, you acknowledge and consent that when you access DoD Information Systems (IS) and Wireless Device (WD):
- a) You are accessing a U.S. Government (USG) IS (which includes any device attached to this IS) or WD that is provided for USG authorized use only.
 - b) You consent to the following conditions:
 1. The USG routinely intercepts and monitors communications on IS for purposes of including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 2. At any time, the USG may inspect and seize data stored on a IS or WD.
 3. Communications using, or data stored on IS or WD are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
 4. IS and WD includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
 5. Notwithstanding the above, using an IS or WD does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 6. Nothing in this User Agreement shall be interpreted to limit the user’s consent to, or in any other way restrict or affect, any USG actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an IS or WD, regardless of any applicable privilege or confidentiality.
 7. The user consents to interception / capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception / capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 8. Whether any particular communication or data qualifies for the protection or a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an IS or WD if the user intends to rely on the protections of a privilege or confidentiality.
 9. Users should take responsible steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user’s identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 10. A user’s failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the USG is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 11. These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the USG shall take reasonable measures to protect the content of captured / seized privileged communications and data to ensure they are appropriately protected.
 12. In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communication and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the USG may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the USG’s otherwise-authorized use or disclosure of such information.
 13. All of the above conditions apply regardless or whether the access or use of an information system includes the display of a Notice and Consent Banner (“banner”). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

6) Unclassified information processing.

The NIPRNET (NGNC Network) is the primary unclassified information system for the NGNC. The NGNC Network is a US-only system.

- a) The NGNC Network provides sensitive but unclassified (SBU) communication to external DOD and other United States Government organizations. Primarily this is done via electronic mail and Internet Networking protocols such as web, FTP, Telnet.
- b) The NGNC Network is approved to process UNCLASSIFIED but SENSITIVE information in accordance with JFHQ-NC PAM 25-1.
- c) The NGNC Network and the Internet, as viewed by the NGNC, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NGNC Network and Internet.

7) Minimum security rules and requirements. Personnel are not permitted access to the NGNC Network unless in complete compliance with AR 25-2 and associated Best Business Practices (BBP). As a NGNC Network system user, the following minimum security rules and requirements apply:

- a) Personnel are not permitted access to NGNC Network unless in complete compliance with AR 25-2.
- b) I have completed the user security awareness-training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification and non-standard threats such as social engineering) before receiving system access.
- c) I will use Common Access Card logon unless I am granted a waiver for another identification method. If User ID / Password is authorized I will ensure my password meets the complexity and length requirement specified by the Information Assurance Manager (IAM).
- d) I will not attempt to access or process data exceeding my authorized Information Security classification level. Computers connected to the NIPRNET are not authorized for the use of classified information.
- e) I understand that I am responsible for any and all activity that occurs under my assigned account. I will not share logon credentials with anyone. I will not store passwords, PINs or other logon credentials on any processor, microcomputer, magnetic, or electronic media - unless such storage is approved in writing by the IAM.
- f) I will generate, store and protect my passwords or pass-phrases. Passwords will consist of at least 10 characters with two each of uppercase, lowercase letters, numbers and special characters. I am the only authorized user of this account. (I will not use my User ID, common names, birthdays, phone

numbers, military acronyms, call signs or dictionary words as passwords or pass-phrases.)

- g) I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs or .bat files) or install programs without authorization, nor will I write / create malicious code or viruses.
- h) I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware or public domain software.
- i) I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment or compact disk.
- j) I will not alter, change, configure or use operating systems or programs, except as specifically authorized by J6 personnel.
- k) I will not utilize Army or DOD-provided IS for commercial financial gain or illegal activities.
- l) Maintenance and upgrades will be performed by the Information Management Officer / Information Assurance Support Officer (IMO / IASO) or designated J6 representative only.
- m) If assigned as an IMO / IASO, I will complete the required IASO certification course.
- n) I will use screen locks and log off the workstation when departing the area.
- o) For standalone classified workstation users, I will immediately report any loss, regardless of duration, to my S2 and / or IASO.
- p) I will immediately report any suspicious output, files, shortcuts or system problems to the J6 Systems Administrator and / or IASO and cease all activities on the system.
- q) I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.
- r) I have received training on Personally Identifiable Information (PII) and understand that I am responsible for safeguarding that I may have access to incident to performing my official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard PII.

- s) I will address any questions regarding acceptable use or information assurance to the J6 Information Assurance Branch.
- t) I understand that monitoring of NGNC Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. DOD policy states that Federal Government communication systems and equipment (including government owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only. I understand that the following activities define unacceptable uses of an Army IS:

1. Sending proprietary, classified or unreleased information to external persons or systems using any electronic means (e-mail, instant messenger, VTC, etc.)
2. Sending unsolicited advertisements, hoaxes or chain mail from an Army IS. Intentionally sending, storing, or propagating sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications. (LE / CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.)
3. Sharing usernames or passwords to the NGNC Network or sharing sessions with authorized or unauthorized personnel (letting someone use your computer while you are logged onto it).
4. Any personal use of government resources involving: copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); pornography or obscene material, gambling; the transmission of chain letters; unofficial advertising, auction web sites soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.
5. Deliberately bypassing security measures such as using personal web based e-mail or connecting a networked system to another network with a modem or providing a backdoor to a system or network or program.
6. Failure to comply with DOD, DA, NGB or NGNC regulations or policies that cover information systems and data handling.
7. Violations will result in the following:

1st Offense: Account disabled, first commissioned officer in chain of command (CoC) must contact J6 Helpdesk to reinstate.

2nd Offense: Account disabled, AO or deputy chief must contact J6 Helpdesk to reinstate.

3rd Offense: Account disabled, first officer in CoC must contact, through CoC, the Chief of Staff to have account re-enabled.

- u) The authority for soliciting your social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to NGNC Network.

8) SIPRNET and Classified Processing – Conditions and Understanding. All of the conditions for access and use of the NGNC NIPRNET also apply to the NGNC SIPRNET and include the following additional conditions.

- a) The SIPRNET is the transport vehicle for processing classified information at the U.S. SECRET classification level. Unauthorized disclosure of SECRET information could reasonably be expected to cause serious damage to the national security of the United States. In accordance with Executive Order (E.O.) 12958, and the National Security Act of 1950, network users are required to protect classified information from any unauthorized disclosure using appropriate safeguards.
- b) Only U.S. Government personnel and contractors with at least a valid SECRET security clearance and need-to-know are allowed access to this network. Access to this network by foreign nationals and other unauthorized personnel is strictly prohibited.
- c) No information will be entered into the SIPRNET or any system on SIPRNET that has a higher classification than U.S. SECRET. Information that is proprietary, contractor-excluded, or otherwise needs special protection or safeguards such as SCI, SPECAT, CNWDI, or SIOP-ESI cannot be entered into the system.
- d) Information classified as CONFIDENTIAL or SECRET may not be stored, processed, or transmitted on the North Carolina National Guard NIPRNET.
- e) Any removable media and printed hardcopy material used on, or derived from the SIPRNET must be marked, stored, handled, and protected at the SECRET classification level regardless of the implied classification level of the data. A dispute over the classification level of data must be resolved by an approved process or declassification authority. (This excludes data and media that already contains an explicit classification label or marking).
- f) SIPRNET workstations, and any associated removable media will not be removed from their approved operating area without the approval of the IAM, or the local commander.

- g) SIPRNET USERID's are considered UNCLASSIFIED / FOUO. SIPRNET passwords are classified SECRET, they must be memorized and never written down and stored.
 - h) Transport of any classified material or system must be accompanied by a valid courier card holder.
- 9) I understand that a violation of these requirements may result in the immediate suspension of my account(s), and that I may be subject to disciplinary, administrative, contractual, NC Code of Military Justice or other prosecutorial actions as applicable.
- 10) **Acknowledgement.** I have read the above requirements (front and reverse) regarding use of the NGNC Network as well as use of classified data processing and SIPRNET. I understand my responsibilities regarding these systems and the information contained in them.

By digitally signing this document, I am legally certifying that I have read, understand and accept my responsibilities under the Acceptable Use Policy. My digital signature is a legally binding signature that ensures the integrity and non-repudiation of my intent to sign this AUP.