NCNG NETWORK ACCEPTABLE USE POLICY (UNCLASSIFIED)

Prescribing Publication: JFHQ-NC REG 25-1 Proponent: JFHQ-NC-J6

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained in NCNG Network from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

2. Access. Access to these Networks 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. **Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. **Unclassified information processing.** The NCNG Network is the primary unclassified information system for the N.C. National Guard. The NCNG Network is a US-only system.

a) The NCNG 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 NCNG Network is approved to process UNCLASSIFIED but SENSITIVE information in accordance with JFHQ-NC PAM 25-1.

c) The NCNG Network and the Internet, as viewed by the N.C. National Guard, are synonymous. E-mail and attachments are vulnerable as they traverse the NCNG Network and Internet.

5. **Minimum security rules and requirements.** As a NCNG Network system user, the following minimum security rules and requirements apply:

a) 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.

b) 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.)

c) I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware or public domain software.

d) I will use virus-checking procedures before uploading or accessing information form any system, diskette, attachment or compact disk.

e) I will not attempt to access or process data exceeding the authorized IS (Information System) classification level.

f) I will not alter, change, configure or use operating systems or programs, except as specifically authorized by J6 personnel.

g) I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs or .bat files) without authorization, nor will I write malicious code.

h) I will safeguard and mark with the appropriate classification level all information created, copied, stored or disseminated for the IS and will not disseminate it to anyone without a specific need to know.

i) I will not utilize Army or DOD-provided IS for commercial financial gain or illegal activities.

j) Maintenance and upgrades will be performed by the Information Management Officer/Information Assurance Security Officer (IMO/IASO) or designated J6 representative only.

k) If assigned as an IMO/IASO, I will complete the required IASO certification course.

l) I will use screen locks and log off the workstation when departing the area.

m) I will immediately report any suspicious output, files, shortcuts or system problems to the J6 SA and/or IASO and cease all activities on the system.

n) I will address any questions regarding this policy, responsibilities, and duties to the J6 Helpdesk and/or IASO.

o) 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.

p) I understand that monitoring of NCNG 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:

- Sending proprietary, classified or unreleased information to external persons or systems using any electronic means (e-mail, instant messenger, VTC, etc…).
- 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.)
- Sharing usernames or passwords to the NCNG Network or sharing sessions with authorized or unauthorized personnel (letting someone use your computer while you are logged onto it).
- 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.
- 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.
- Failure to comply with DOD, DA, NGB or NCNG regulations or policies that cover information systems and data handling.
- 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.

6. Acknowledgement. I have read the above requirements (front and reverse) regarding use of the NCNG Network. I understand my responsibilities regarding these systems and the information contained in them.

Section/Unit/MACOM	Date
Last Name, First, MI	**Rank/Grade**
Signature	**Phone Number**