# DMA/KYARNG ACCEPTABLE USE POLICY (AUP)

For use of this form, see AR 25-2; the proponent agency is NGKY-IMA-IA

*Reference: AR 25-2 (Information Assurance). A well-protected Department of Defense (DoD) or Department of the Army (DA or Army) network enables organizations to easily handle the increasing dependence on the Internet. For a DoD/Army organization to be successful, it needs to integrate information that is secure from all aspects of the organization. The purpose of this policy is to outline the acceptable use of computer equipment within the Kentucky National Guard (KYARNG) and the Kentucky Department of Military Affairs (DMA). These rules are in place to protect the employee and the organization. Inappropriate use exposes KYARNG units and the DMA to risks including attacks, compromise of network systems and services, and legal issues. This policy applies to all employees, contractors, consultants, temporary employees, and other workers assigned to the KYARNG or DMA. All Information Technology (IT) assets, devices, and services that connect or utilize network resources are covered by this Acceptable Use policy (AUP) and all applicable Commonwealth of Kentucky policies or Kentucky Revised Statutes (KRS) legislation.*

**1. Understanding.** I understand that I have the primary responsibility to safeguard the information contained in the information contained in the Non-secure Internet Protocol Router Network (NIPRNET) from unauthorized or inadvertent use, modification, disclosure, destruction, and denial of service. This includes all network resources of DMA.

**2. Access.** Access to this network is for official use and authorized purposes and as set forth in DOD Directives 5507.7-R Joint Ethics Regulation (JER), AR 25-2 (Information Assurance) and Army/ARNG/DMA network policy and accreditation.

**3. Revocability.** Access to Army/ARNG/DMA Information Systems resources is a revocable privilege and is subject to content monitoring and security testing.

**4. Unclassified information processing.** The NIPRNET is the primary unclassified information system for Army units. NIPRNET provides unclassified communication to external DoD and other United States Government organizations. Primarily, this is done via electronic mail and Internet networking protocols such as Web Access, Virtual Private Network, or other approved remote access system.

a. NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2 and local automated information system security management policies. A Designated Approval Authority (DAA) has accredited this network for processing this type of information.

b. The NIPRNET and the Internet, for the purpose of the AUP, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet, as well as all inbound/outbound data, external threats (e.g. worms, denial of service, hacker) and internal threats.

c. Public Key Infrastructure (PKI) Use:

(1) Public Key Infrastructure provides a secure computing environment utilizing encryption algorithms (Public/Private-Keys).

(2) Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is now the primary access control mechanism for all Army users (with very few exceptions). This is a two phase authentication process. First, the CAC is inserted into a middleware (reader), and then a unique user PIN number provides the validation process.

(3) Digital Certificates (Private/Public Key). CAC is used as a means to send digitally signed e-mail and encrypted e-mail.

(4) Private Key (digital signature), as a general rule, should be used whenever e-mail is considered "Official Business" and contains sensitive information (such as operational requirements). Additionally, all emails with embedded hyperlinks and or attachments must be digitally signed. The digital signature provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail.

(5) Public Key is used to encrypt information and verify the origin of the sender of an email. Encrypted mail should be the exception, and not the rule. It should only be used to send sensitive information, information protected by the Privacy Act of 1974, and Information protected under the Health Insurance Portability and Accountability Act (HIPAA), or identified as For Official Use Only (FOUO).

(6) Secure Socket Layer (SSL) technology should be used to secure a web based (https) transaction.

DoD/Army Private (Intranet) web servers will be protected by using this technology IAW DoD/Army PKI implementation guidance.

**5. User Minimum-security rules and requirements.** As a NIPRNET system user, the following minimum-security rules requirements apply:

a. I understand personnel are not permitted access to the NIPRNET unless they have met the appropriate DOD and Army personnel security requirements for accessing the system.

b. I have completed the required security awareness-training (Annual DoD Information Assurance Awareness Training or Computer Security for Users) and provided proof of completion to my Information Assurance Support Officer (IASO). IAW AR 25-2, prior to receiving network/system access, I will participate in all DoD/Army/ARNG/DMA sponsored Security Awareness Training and Certification programs inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering. I understand that my initial training certificate will expire one year from the date that I successfully complete training and that I will be required to complete annual refresher training (IAW AR 25-2). I understand that my account will be disabled if I do not complete the annual certification training by the anniversary date.

c. I will protect my logon credentials (passwords or pass-phrases). Passwords will consist of at least 14 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of my 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. IAW AR 25-2, Chapter 4, Section IV, Para 4-12, passwords should be changed at least every 60 days.

d. When I use my CAC to logon to the network, I will ensure it is removed and I am logged off prior to leaving the computer.

e. I will use only authorized hardware and software on the DoD/Army networks to include wireless technology. I will not install or use any personally owned hardware (including removable drives), software, shareware, or public domain software unless specifically approved the Kentucky J6/DOIM.

f. To protect the systems against viruses or spamming, I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, compact disk, or other storage media.

g. I will not attempt to access or process data exceeding the authorized IS classified level.

h. I will not alter, change, configure, or use operating systems, programs, or information systems except as specifically authorized.

i. 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.

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

k. I will not utilize DoD/Army/ARNG/DMA provided IS for commercial financial gain or illegal activities.

l. Maintenance will be performed by the System Administrator (SA) only.

m. I will use screen locks or log off the system when departing the area.

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

o. I will address any questions regarding policy, responsibilities, and duties to my IASO and/or the Kentucky J6 Helpdesk.

p. I understand that each Information System (IS) is the property of the Army and is provided to me for official and authorized use.

q. I understand that monitoring of NIPRNET will be conducted for various purposes and information captured during monitoring may be used for possible adverse administrative, disciplinary or criminal actions. I understand that the following activities are prohibited uses of an Army IS:

(1) Unethical use (e.g. Spam, profanity, sexual misconduct, gaming, extortion).

(2) Accessing and showing unauthorized sites (e.g. pornography, E-Bay, chat rooms).

(3) Accessing and showing unauthorized services (e.g. peer-to-peer, distributed computing)

(4) Unacceptable use of e-mail includes exploiting list servers or similar group broadcast systems for purposes beyond intended scope to widely distribute unsolicited e-mail (SPAM); sending the same e-mail message repeatedly to interfere with recipient's use of e-mail; sending or broadcasting, e-mail messages of quotations, jokes, etc., to multiple addressees; and sending or broadcasting unsubstantiated virus warnings (e.g. mass mailing, hoaxes, auto-forwarding) from sources to anyone other than the IAM.

(5) Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is unacceptable use (e.g., video, sound or other large files, "push" technology on the internet and other continuous data streams).

(6) Unauthorized sharing of information that is deemed proprietary or not releasable (e.g. use of keywords, phrases or data identification).

r. I understand that I may use an Army IS for limited personal communications by e-mail and brief internet searches provided they are before or after duty hours, break periods, or lunch time or IAW local policies and regulations, as long as they do not cause an adverse impact on my official duties; are of reasonable duration, and cause no adverse reflection on DOD. Unacceptable use of services or policy violations may be a basis for disciplinary actions and denial of services for any user.

s. I understand that AR 25-2 is the implementation of Federal Law and is punitive in nature. Violations of paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5 of this regulation may be punishable as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. Personnel not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative, or prosecutorial actions.

6. By signing this document, I acknowledge and consent that when I access Department of Defense (DOD) information systems:

a. I am accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

b. I consent to the following conditions:

(1) The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct, law enforcement (LE), and counterintelligence (CI) investigations.

(2) At any time, the U.S. Government may inspect and seize data stored on this information system.

(3) Communications using data stored on U.S. Government information systems are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

(4) This information systems includes security measures (e.g., authentication and access controls) to protect U.S. Government interests; not for my personal benefit or privacy.

(5) Notwithstanding the above, using an information system 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 on page 3:

(a) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

(b) The user consents to interception/capture and seizure of all communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counter-intelligence 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

(c) Whether any particular communication or data qualifies for the protection of 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, if the user intends to rely on the protections of a privilege or confidentiality.

(d) Users should take reasonable 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.

(e) 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 U.S. Government 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.

(f) 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 U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

c. 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 communications 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 U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

d. All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent 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.

**7. Remote access.** Remote access will be via virtual private network (VPN). Government owned hardware and software will be used. The employee is the only individual authorized to use this equipment. Access will be as authorized by the supervisor. Requirements as indicated throughout this AUP are applicable for access to USG resources.

**8. "Road Warrior" Laptop Security.** Users of mobile computing devices (laptops, portable notebooks, tablet-PCs, and similar systems) are tasked with the physical security of these mobile devices while administrators must protect the IS from compromise when used as a standalone system or when remotely connected. I have read and understand the BBP, "Road Warrior" Laptop Security (found on the https://informationassurance.us.army.mil website).

I understand that AR 25-2 is the implementation of Federal Law and is punitive in nature. Violations of paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5 of this regulation may be punishable as violations of a lawful general order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable. Personnel who are not subject to UCMJ who fail to comply with these requirements may be subject to disciplinary, administrative, or prosecutorial actions.

**9**. **Privileged Users.** When logged in as a privileged user (using an administrative account), I will not use applications that access the Internet (such as web browsers) or applications with potential Internet sources (such as email) except as necessary for local service administration.

## Reporting

If system compromise is suspected, disconnect the LAN cable and discontinue use. You should leave the system powered on. Do not click on any prompts or close any open windows. Write down all actions that occurred during the suspected attack (ex. if a message appears on the monitor of the affected system). Notify your IASO or supervisor immediately.

Some examples of possible system compromise are:

(1) Known or suspected intrusion or access by an unauthorized individual.
(2) Authorized user attempting to circumvent security procedures or elevate access privileges.
(3) Unexplained modifications of files, software, or programs.
(4) Unexplained or erratic IS system responses.
(5) Presence of suspicious files, shortcuts, or programs.
(6) Malicious logic infection (for example, virus, worm, Trojan).
(7) Receipt of suspicious e-mail attachments, files, or links.
(8) Spillage incidents or violations of published BBP procedures.

Data Compromise/Spillage is the unintentional release of secure information to an unsecure environment. Report all incidents immediately by telephone or in person to your Supervisor, IASO, IMO and/or the J6 Helpdesk.

## When to sign and/or encrypt E-mail

PKI Digital Encryption - Use DOD PKI certificates to encrypt e-mails containing For Official Use Only, Privacy Act and Personally Identifiable Information; individually identifiable health information; and other sensitive, but unclassified information.

PKI Digital Signature - Use digital signatures whenever it is necessary for the recipient to be assured of the sender's identity, have confidence the message has not been modified or when non-repudiation is required.

## Best Business Practices

Maintain physical control of your CAC card at all times. Do not share your CAC PIN with anyone.

Be cautious of emails containing attachments or links. Notify the J6 Helpdesk of any email you feel may be malicious.

Back up your important data regularly using the KYNG Backup User Application. Data backup is the responsibility of the user.

☐ ***My initials indicate that I have read all pages and agree to the terms and conditions of the DMA/KYARNG Acceptable Use Policy***

| | |
|---|---|
| Last Name, First Name, MI | Rank/Title |
| MACOM UNIT OF ASSIGNMENT | SSN: Last four digits |
| Area Code and Phone Number | Signature |