

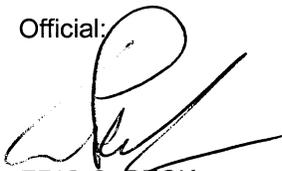
Information Management

INFORMATION ASSURANCE PROGRAM

By Order of the Adjutant General:

JONATHAN P. Small
Brigadier General, KSARNG
Commander, KSARNG

Official:



ERIC C. PECK
COL, GS, KSARNG
Chief of Staff

Summary. This regulation prescribes procedures for securing Information Systems (IS), which is any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and that includes computer software, firmware, and hardware. Included are computers, word processing systems, networks or other electronic information handling systems and associated equipment.

Applicability. This regulation applies to the office, as a State agency and a military headquarters (Hqs), Joint Forces HQ

Supplementation. This regulation may be supplemented. Supplement must be coordinated with the Joint Forces Headquarters (JFHQ)J6 (Command, Control, communications, and computers)

Exceptions and waivers. Exceptions and waivers to this SOP must be in writing for each system covered. Items covered in Regulations and higher cannot be waived.

Interim Changes. Interim changes to this regulation are not official unless authenticated by the J6. Interim changes will be destroyed on their expiration dates unless sooner rescinded or superseded.

Suggested Improvements. The proponent of this regulation is the J6. Users are invited to send comments and suggested improvements directly to J6 KSARNG, 2800 SW Topeka Blvd, Topeka, Kansas 66611-1287.

Distribution. A

	Paragraph	Page
Chapter 1 - General		
Purpose	1-1	1
Objectives	1-2	1
Responsibilities	1-3	1
Chapter 2 - KSNG Information Assurance Policy		
General Policies	2-1	3
Descriptions and Definitions	2-2	4
User Policies	2-3	4

	Paragraph	Page
Hardware Policies	2-4	6
Minimum Information Assurance requirements	2-5	6
Remote Access	2-6	8
Configuration Requirements	2-7	8
Virus Protection	2-8	8
Password Controls	2-9	9
Tactical Systems	2-10	10
Maintenance	2-11	10
Security Considerations	2-12	10
Chapter 3 – Accreditation		
Accreditation Process	3-1	11
Chapter 4 – Personnel Security		
Personnel Security	4-1	12
Personnel Security Investigation and Clearance	4-2	12
Personnel Security Training	4-3	12
Chapter 5 - Classified Processing on Personal Computers		
Security Guidance	5-1	13
Classified Processing Procedures	5-2	13
Chapter 6 – Software Controls		
Software Acquisition	6-1	14
Software Control Procedures	6-2	14
Procedures for Safeguarding Software	6-3	14
Chapter 7 – Incident Reporting		
Incident and Intrusion Reporting.	7-1	15
Reporting Responsibilities	7-2	15
ANNEXES		
A. IASO Appointment Letter		18
B. User Policy Letter		19
C. Incident Response Form		20
D. NGB Acquisition Policy		21
E. Sample Accreditation Letter		22
F. IASO Binder Tabs		23
G. Inspection Checklist		24

CHAPTER 1 - GENERAL

1-1. Purpose. This regulation provides guidance for security assurance of information belonging to the Army, as well as sensitive personal information.

1-2. Objectives. The objective of this regulation is to provide uniform procedures to:

- a. Allow access to information systems (IS).
- b. Ensure the required IS, training, and equipment are given to personnel.
- c. Ensure KSARNG compliance with current National Guard Bureau (NGB), Army, DOD regulations and directives.

1-3. Responsibilities.

a. To provide the most efficient application of the KSARNG IS program, the following responsibilities are assigned:

(1) JFHQ J6:

- (a) Provides approval of staff/unit IT requirements in accordance with AR 25-1.
- (b) Provide assistance in procuring and using hardware and software.
- (c) Assist functional personnel in formulating applications for the AIS and solving technical problems.
- (d) Provide technical advice for IS activities.
- (e) Research and develop microcomputer standards to ensure compatibility.
- (f) Assist the staff and units in developing AIS requirements for their respective areas.

(g) Advise and assist staff sections and units in regard to security and accreditation requirements.

(2) Staff and units (Division, Brigade (BDE), Battalion (BN) or directorates): Designate an Information Assurance Officer (IASO). An Alternate IASO will be designated and perform the duties of the IASO when the primary is not available for duty. This IASO will: (See App A-1 for appointment memorandum format)

(a) Serve as the interface between the functional user/unit and the higher headquarters (Hqs) IASO for all IT activities.

(b) Notify the J6 immediately of any problems encountered with the AIS (e.g., software, communications, etc.)

(c) Request additional hardware/software in accordance with procedures identified in paragraph 2-2.

(d) Provide resource management by:

[1] Routinely powering up and down the system to meet user needs as well as data patch level and maintenance.

[2] Adding and removing terminals, printers, microcomputers and other peripheral equipment as it becomes necessary for the optimizing and efficient use of system resources.

[3] Insuring all users are documented, have a "need to know" on the information they are accessing, and have a clearance commensurate with the level of work being done.

[4] Insuring all users are briefed on security measures and all regulations pertaining to proper operations of equipment handling highly sensitive data.

[5] Taking care to use proper physical security by measures on the equipment to protect the equipment from theft or vandalism, which will reduce the chances of unauthorized attempts at system access.

[6] Maintain a list of computers, peripherals, and users under their control.

[7] Provide user assistance and training by:

[a] Determining what assistance and training is needed by users. The IASO will be normally considered the "technical advisor" to the Commander's/Staff Directorate. Day-to-day oversight and coordination with the end users of the system will allow for developing training and assistance requirements to effectively support the users of the system.

[b] Formally requesting needed training classes to the J6 far enough in advance to allow for proper budgeting and scheduling, normally 90 days in advance for training required and 30 days in advance of assistance needed.

[c] Providing for a documented on-the-job training (OJT) program for new employees until they are able to attend formal classes on the system.

CHAPTER 2 - KSARNG INFORMATION ASSURANCE POLICY

2-1. General Policies.

a. The J6 has the final authority to approve AIS resources in response to mission needs that cannot be economically satisfied by current automation capabilities and which do not duplicate or alter the configuration of existing application systems. Software acquired in support of the above referenced functions will not duplicate present or planned Army Standards Systems or existing KSARNG automated systems. Additionally, newly acquired AIS will be compatible with currently installed microcomputer systems. Any automation equipment that either directly or indirectly connects to the KSNG LAN must be approved in writing from the J6.

b. Training and using off-the-shelf software is the responsibility of functional users. Other than web pages and database applications, custom designed programs will not, as a general rule, be developed by J6 nor will the J6 provide maintenance support or training for functional user developed programs.

c. Access to other KSARNG system/data. An AIS with dial-up communications capabilities functions as a computer terminal when accessing another computer system. PCs will not access the KSARNG Intranet without prior approval from the J6. This includes personally owned computers connecting from homes.

d. Classified or Privacy Act Information.

(1) Classified Information: Classified information is not authorized for processing on the AIS without prior approval of the Information Assurance Manager (IAM) KSARNG. The accreditation document will include classified processing considerations. Classified information will only be processed on computers that are accredited for the level of classification required.

(2) Personnel Data: All users must safeguard systems with personnel data according to the Privacy Act of 1974, Public Law 93-597, and Title 5 USC.

e. Software Piracy.

(1) Laws. Users will read and comply with the software license agreements. This includes prohibitions against copying materials (media and manuals) legally protected by copyrights and using software on more than one PC. If multiple copies are needed they must be purchased. It is against the law to copy/reproduce computer programs. Limitations and restrictions are imposed by the copyright license agreement of each program. This prohibition includes not only copying for personal use but also copying for use in legitimate applications.

(2) Shareware. Software distributed under the "Shareware Concept" is still copyrighted and requires purchasing a license to use. Shareware software is not FREE or the same as Public Domain software. Shareware will not be installed on government owned computers unless purchased by the J6.

(3) Public Domain. Software in the Public Domain is the only software that may be used and freely copied without restriction or limitations normally imposed by copyright licensing agreements. This software must still be approved in writing by the J6. Requests are to be submitted in writing to either the J6 or the helpdesk.

(4) Copying. Some licenses allow a user a backup or archival copy to have on hand in case the program media is damaged. Making copies to share with other computer users, or copying a program at work to use at home, is forbidden.

f. Privately Owned Computers. The connection of privately owned computers to the KSNG LAN is strictly forbidden. There will be no government sensitive information on personally-owned systems.

g. Personal Use of Government Owned Computers. The government provides computer resources for the accomplishment of official duties. The use of government owned computers in support of private/personal programs/endeavors is expressly forbidden. Such programs/endeavors is defined to include personal use, use by clubs or other organizations, companies, games, or any other activity, which does not specifically support the daily conduct of business for the Kansas Army National Guard. Violations will be reported through the IASO to the IAM.

2-2. Descriptions and Definitions.

a. Automated Information System (AIS, also called IS).

(1) An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information.

(2) Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware (Note: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment).

b. Network. Two or more AIS connected.

c. SECRET Internet Protocol Router Network (SIPRNET). The Department of Defense Network that is accredited SECRET (S).

d. Non-Secure Internet Protocol Router Network (NIPRNET). The Department of Defense Network that is accredited Sensitive but unclassified.

e. Local are Network (LAN). A network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

f. Wide Area Network (WAN). A Network that spans a relatively large geographical area. Typically a WAN consists of two or more local-area networks (LANs).

2-3 User Policies. *General users.* Users must have a favorable background investigation or hold a security clearance or access approvals commensurate with the level of information processed or available on the system.

a. User requirements.

(1) Comply with the guidelines established under the DOD 5500.7 when making personal use of government-owned ISs.

(2) Participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

(3) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them and with a valid need to know.

(4) Protect ISs and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(5) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network, as outlines in the acceptable use policy (AUP) letter that all users must sign (see annex B).

(6) Safeguard and report any unexpected or unrecognizable output products.

(7) Report the receipt of any and all media (for example, CD-ROM, floppy disk) received to the IAM or system Administrator (SA), as appropriate, for authorization to use.

(8) Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the IS.

(9) Report all known or suspected security incidents, spam, chain letters, and violations of access through Information assurance channels (IASO to IAM).

(10) Comply with password or pass-phrase policy directives and protect passwords from disclosure.

(11) Logoff ISs at the end of each workday.

(12) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need to know, and assume only authorized roles and privileges.

b. Prohibited activities. The following activities are specifically prohibited:

(1) Use ISs for personal commercial gain or illegal activities.

(2) Use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct.

(3) Intentionally send, store, or propagate the following types of communications:

a. Sexually explicit

b. Threatening

c. Harassing

d. Political

e. Unofficial public activity (that is, spam)

(4) Participate in on-line gambling or other activities inconsistent with public service.

(5) Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

(6) Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring.

(7) Modify system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications).

(8) Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.

(9) Share personal accounts and passwords.

(10) Disable or remove security or protective software or mechanisms and their associated logs.

c. Acceptable Use Policy (AUP).

(1) Users will be advised that there is no expectation of privacy while using Army ISs or accessing Army resources except with respect to LE/CI activities.

(2) Users must review and acknowledge this AUP (see Annex B) and IASOs will maintain documented records.

(3) 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.

(a) Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a theater commander for soldiers and civilian employees deployed for extended periods away from home on official business.

(b) Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes.

(c) Authorized purposes can also include individuals from the DSCIM with the technical expertise to detect unauthorized modifications and will monitor all uncleared maintenance personnel.

2-4. Hardware Policies.

a. Organic computers will at a minimum:

(1) Not show the last user to use the system.

(2) Belong the KS active directory domain.

(3) Be a client of the Software Update Server.

(4) Be a client of the Systems Management Server.

(5) Have a warning banner before the login screen.

(6) Be a client of the anti-virus server.

(7) Not have a firewall enabled.

(8) Not have any civilian ISP software installed (AOL, Earthlink, etc)

(9) Not have any "file sharing" software installed (Kazaa, Limewire, etc)

(10) Not have any "chat software installed. (ICQ, Yahoo IM, etc) AKO IM is the only authorized chat software.

(11) Not have a generic user id (student, user1, etc).

(12) Will be fully compliant of all Information Assurance Vulnerability Alerts.

b. Inorganic Computers. These systems contain those belonging to contractors or other entities that are connected to the .mil network for government-related work. They will at a minimum:

- (1) Have a signed interim authority to connect from the J6.
 - (2) Have antivirus software installed and the definition files will not be more than one week old.
 - (3) Not have any "file sharing" software installed
 - (4) Be scanned for vulnerabilities before connection
 - (5) Not have a firewall enabled
- c. Personally owned computers will not connect to the .mil network

2-5. Minimum Information Assurance Requirements.

a. Configure ISs to implement the principle of least privilege through automated or manual means. All risk analyses will evaluate possible vulnerabilities and adverse security effects on the associated ISs and networks within the appropriate areas of responsibility. Although manual procedures are acceptable when an automated safeguard is not feasible, embed automated security safeguards into the design and acquisition of new or updated ISs to ensure a secure infrastructure. Employ technical capabilities to achieve these requirements to the greatest extent possible.

b. Access Control. Implement controls to protect ISs from compromise, unauthorized use or access, and manipulation. IA personnel will immediately report unauthorized accesses or attempts of such systems.

- (1) Access to Army ISs or networks is a revocable privilege.
- (2) Approval processes will be developed and determined for specific groups and users.
- (3) Individuals will meet security investigation (or approved interim access) requirements before IS access.
- (4) Systems will automatically generate an auditable record or log entry for each access granted or attempted.
- (5) Identify all users through a unique user identification (USERID).
- (6) Authenticate user access to all systems with a minimum of a USERID and an authenticator. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.
- (7) Use password-protected screen savers, screen locks, or other lockout features to prevent unauthorized access on all ISs during periods of temporary non-use; configure such mechanisms to automatically activate when a terminal is left unattended for no longer than 10 minutes. Establish a shorter period if appropriate, such as in a multinational work area.
- (8) The use of group accounts is generally prohibited. Permit exceptions only on a case-by-case basis that support an operational or administrative requirement such as watch-standing or helpdesk accounts, or that permit continuity of operations, functions, or capabilities. IAMs will implement procedures to identify and audit users of group accounts through other operational mechanisms such as a duty logs.
- (9) Implement a policy of least privilege for access to system resources or information.

(10) Limit the number of user failed log-on attempts to three before denying access to (locking) that account, when supported by the IS or device. If IS-supported, the system will prevent rapid retries when a password is incorrectly entered and gives no indications or errors that either the password or ID was incorrectly entered (for example, implement time delays between attempts).

(11) A security alert will be generated and investigated when the maximum number of password attempts is exceeded, the maximum number of attempts from one IS is exceeded, or the maximum number of failed log-ins over a period is exceeded.

(12) Reinstate accesses only after the appropriate IA (for example, SA/NA) personnel have verified the reason for failed log-on attempts and have confirmed the access-holder's identity. Permit automatic account unlocking (for example, established time period elapsed) as an exception only, based on sensitivity of the data or access requirements.

(13) Implement mandatory audit trails to record all successful and unsuccessful log-on attempts.

(14) Temporarily disable all accounts for deployed forces on garrison networks unless operationally required.

(15) Implement procedures for suspending, changing, or deleting accounts and access privileges for deployed forces in the event of capture, loss, or death of personnel having network privilege-level access.

(16) Enable, log, and protect physical access control events (for example, card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts as required.

2-6. Remote Access.

a. Any IS being used for remote access will employ host-based security and AV software before authorization to connect to any remote access server.

b. Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

c. Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

d. Users will protect RA ISs and data consistent with the level of information retrieved during the session.

e. Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

f. Remote access users will read and sign security and end-user agreements for remote access annually as a condition for continued access.

g. Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable dial-in modems.

2-7. Configuration Requirements. The following policy will be the minimum used for the configuration management of all systems.

a. Hardware and software changes to an accredited IS with an established baseline will be effected through the configuration management process.

b. The CCB or the Configuration Management Board (CMB) for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without the express written consent of the IAM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate commander or manager will provide the consent on the advice of the cognizant IA official.

2-8 Virus Protection. Implement the virus protection guidance provided below on all ISs and networks, regardless of classification or purpose.

a. Scan all files and software, including new "shrink-wrapped" Commercial Off the Shelf (COTS) software, with an AV product before introducing them onto an IS or network.

b. To minimize the risks of viruses, implement the following countermeasures.

(1) Ensure all ISs have a current and supportable version of the AV software configured to provide real-time protection.

(2) Install an AV product for every remote access IS.

(3) IA personnel should take the multilevel approach to virus detection by installing one AV package on the workstations and a different AV package on the servers.

(4) Update virus definitions as a minimum weekly, or as directed by the ACERT for immediate threat reduction. Virus definition availability is based on vendors' capabilities, and IA personnel will institute processes to automatically update definitions as published or available from authorized DOD or Army sites.

(5) Train users to scan all software, downloaded files, and e-mail attachments to prevent malicious logic installation.

(6) Train users to recognize and report virus symptoms immediately.

c. IAMs will implement virus-reporting procedures to support DOD and Army reporting requirements.

2-9. Password Control.

a. The IAM or designee is responsible for overseeing the password generation, issuance, and control process.

b. The holder of a password is the only authorized user of that password.

c. Change passwords on secret accredited systems no less frequently than every 90 days (every 30 days if approved password vault software or devices are utilized) and protect them from disclosure.

d. Configure ISs to prevent displaying passwords in the clear unless tactical operations (for example, heads-up displays while an aircraft is in flight) pose risks to life or limb.

e. Generate passwords as follows:

(1) The minimum requirement is a 10-character case-sensitive password. Passwords or phrases longer than 10 characters are recommended when supported by the IS. Password expiration will be not more than 150 days.

(2) The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters (for example, x\$T!oTBn2!) and can be user generated.

(3) Enforce password policy through implementation or enhancement of native security mechanisms.

(4) Passwords will not include such references as social security account numbers (SSAN), birthdays, USERIDs, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or names; neither will they be easy to guess (for example, mypassword, abcdel2345).

(5) Password history configurations will prevent reutilization of the last 10 passwords when technically possible. IAMs will approve and manage procedures to audit password files and user accounts for weak passwords, inactivity, and change history. Conduct quarterly auditing of password files on a stand-alone, secured system with limited access. Encrypt password files for transit if auditing at a centralized location.

f. Deployed and tactical systems with limited data input capabilities will incorporate password control measures to the extent possible.

g. Implement other authentication techniques (for example, biometrics, access control devices, or smart cards) as viable alternatives in conjunction with, or in place of, passwords as tested or approved by NETCOM and CIO/G-6.

h. Remove or change default, system, factory installed, function-key embedded, or maintenance passwords.

i. Unauthorized scans. Treat unauthorized scans of networks as potential intrusions and report upon detection. Persons conducting unauthorized scans of Army networks may be subject to administrative actions or punishment.

2-10. Tactical Systems.

a. Tactical systems, including weapon system and devices integral to weapon or weapon support systems, that include features normally associated with an IS will implement the requirements of this regulation and Department of Defense Instruction (DODI) 5200.40 Department of Defense Information Technology Security Certification and Accreditation (DITSCAP).

b. When one or more of the minimum-security requirements are impractical or adversely impose risk of safety-of-use because of the function and design of the system, the situation will be addressed in the SSAA as well as in the C&A approval memorandum signed by the DAA.

c. Mechanisms must be available to render the IS inoperable in case of imminent capture by hostile forces.

d. Tactical networks connecting to standard tactical entry point (STEP) sites, garrison, or other fixed networks must be compliant with all security requirements (for example, configurations, approved software,) before connection. They will be protected by access controls and intrusion detection systems in the same manner as garrison network defenses described earlier and will adopt a Defense in Depth (DiD) strategy.

2-11. Maintenance.

a. The IASO will ensure PMCS (such as defrag, fdisk, etc..) will be performed.

b. The J6 will be contacted immediately if there are problems with the software.

c. CSMS will be notified of any hardware problems.

2-12. Security Considerations.

a. General. All computer areas will be secured upon the completion of the duty day or at any time the facility is unoccupied, such as during a fire drill, bomb threat, etc. Only authorized users are allowed to use hardware in conjunction with his/her duties. Double barrier security for AIS should be provided wherever possible.

b. Security of CPU, Printer, and Keyboard. LOCKED doors will secure the system unit keyboard and printer, at a minimum, at the end of the duty day. Computer equipment must be secured by a minimum single barrier security when left unattended.

c. Use of government-owned computers at homes or other facilities is authorized providing the following:

(1) Work on the systems must be for official use only.

(2) No software will be installed to allow connection to the internet (i.e. AOL, SBC-Yahoo, etc)

(3) Anything introduced or produced on the system becomes property of the KSNG.

(4) No IT or IT resources shall be left unsecured.

CHAPTER 3 - ACCREDITATION

3-1. Accreditation Process.

a. Accreditation is the critical review of a designated automated system prior to operation. It will provide the accreditation authority and System Security Manager information to determine that sensitive information can be processed within the bounds of acceptable risk (AR 380-19, 1-4)

b. The accreditation process requires, as a minimum investigation, information gathering, and formal review by management at both the operating and accrediting levels.

c. Since the documentation associated with the formal accreditation describes in detail the vulnerabilities, risks, system design and physical layout of the system, consideration should be given to classifying such documentation at a level commensurate with the classification of information in the system. As minimum, the documentation will be considered "FOR OFFICIAL USE ONLY". Access to accreditation should be on a "need-to-know" basis.

CHAPTER 4 - PERSONNEL SECURITY

4-1. Personnel Security. The Personnel Security and Surety Program (PSSP) will consist of the following:

a. The following positions are designated as levels of authority and requirements..

(1) Information Assurance Program Manager (IAPM) (NGB IA POC)

(2) Information Assurance Manager (IAM) (State IA POC) minimum training requirements:

(a) User training.

[1] IAPM& S course.

[2] Level I (IASO), II (SA/NM course), and III (OTE).

(b) Rights: Conduct vulnerability scans and investigations.

(3) System administrators (those with domain/computer administrative rights) minimum training requirements:

(a) User training.

[1] Level I (IASO),

[2] II (SA/NM course).

(b) Rights: Overall rights to modify software, hardware, and users.

(4) Information Assurance Officer (IASO) (unit IA POC) minimum training requirements:

(a) User training. Level I (IASO),

(b) Rights: Maintain user training/policy files.

(5) Power users (those with application and system change rights) minimum training requirements:

(a) User training. Level I (IASO),

(b) Rights: Repair applications and install drivers.

b. Initial screening and evaluation. All personnel will be screened prior to assignment. The screening will consist of a review of all records relevant to the individual's loyalty and reliability.

4-2. Personnel Security Investigation and Clearance. Those with administrative rights on IS will have a SECRET clearance at a minimum. .

4-3. Personnel Security Training. All users will take and pass the user security training before receipt of a login/password.

CHAPTER 5 - CLASSIFIED PROCESSING ON PERSONAL COMPUTERS

5-1. Security Guidance. This chapter provides security guidance for organizations and individuals using IS. The level of protective measures applied should be commensurate with the environment and sensitivity of information being processed.

a. For the purpose of this guidance AIS includes word processors, personal computers, professional computers, portable, laptop, handheld computers, home computers, desktop computers and multi-user microcomputers.

b. The users of AIS are responsible for the physical security and environmental safeguards for the equipment, media, and data processed.

Properly securing sensitive information and media to protect against unauthorized access, destruction, or damage.

(1) Labeling reports generated to identify and differentiate the sensitivity of information as well as the creator's name and date of processing.

(2) Protecting the computer with the same level of security as the printed copy.

5-2. Classified Processing Procedures.

The IASO will ensure that AIS is properly prepared for processing the level of classified information required.

a. A label or sign should be placed on the computer indicating the highest level, which may be processed.

b. These procedures are intended for use between the levels of classified processing (such as, between SECRET and CONFIDENTIAL) as well as between classified and unclassified. The procedures below must be adhered to when classified defense information is processed:

(1) Ensure that the computer is approved for processing the level of classified information required.

(2) Physically disconnect any communications lines or modems from laptop (handheld) computers. Desktop computers will only have a network card installed and that must be disconnected

(3) Physically disconnect any other resources (i.e., separate hard drive, printer, additional workstations, plotter, etc.) not required during the session (if possible).

(4) Display a placard indicating the classification level of the processing in progress.

(5) Ensure that the power has been turned off prior to initiating the session.

(6) Ensure that the work station screen is positioned to prevent viewing by unauthorized persons.

(7) When the session is complete, remove all media clear the system as described in local procedures, and power down the system.

CHAPTER 6 – SOFTWARE CONTROLS

6-1. Software Acquisition.

- a. Procurement is forbidden of any hardware or software without written J6 approval.
- b. Software Applications. Software applications will not duplicate present National Guard standard applications. The J6 maintains a list of applications. That list will be reviewed before initiating any new development.
- c. Hardware/Software. Efforts must be made to ensure microcomputer hardware/software is standardized and compatible throughout the command. The J6 is responsible for the selection of microcomputer resources (hardware and software) which will be compatible with existing KSARNG IS.
- d. Naming Conventions: Care must be exercised when writing programs to use standard names and formats for data fields. The Army 18 series and functional guidance (ARs, ADSMs, etc.) should be consulted. Proposals for standard data elements should be submitted through functional channels.

6-2. Software Control Procedures. At no time will unapproved or non-authorized software be used on any system. This applies to the following software categories:

- a. Freeware.
- b. Shareware.
- c. Privately procured software.
- d. Pirated software.
- e. "Chat" software other than AKO.

6-3. Procedures for Safeguarding Software.

- a. Government purchased software will be copied for day-to-day use. The original copy will be stored as backup at the J6 unless prohibited by the purchasing agreement.
- b. Original software will be protected from loss or theft by storage in a locked container such as a cabinet, safe, or desk.

CHAPTER 7 – INCIDENT REPORTING

7-1. Incident and Intrusion Reporting.

a. Incidents may result from accidental or deliberate actions on the part of a user or external influence. Evidence or suspicion of an incident, intrusion, or criminal activity will be treated with care, and the IS maintained without change, pending coordination with IA, ACERT/RCERT, and LE/CI personnel. Ensure users are aware of the policy governing unauthorized use of computer resources.

b. Users will report all potential or malicious incidents because time-sensitive actions are required to limit the amount of damage or access. IS incidents will be reported within the command and to external agencies to assist LE or investigative agencies in compiling supporting evidence, impact assessments, associated costs, containment viability, and eradication and reconstruction measures necessary to effectively manage the breach and provide evidentiary material for prosecution.

(1) Protect IS incident reports as a minimum FOUO or to the level for which the system is accredited.

(2) Annually validate IS incident reporting procedures.

c. Report all IS incidents or events including, but not limited to:

(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.

d. A serious incident report (SIR) will be generated and reported per AR 190-40 under the following conditions.

(1) The incident poses grave danger to the Army's ability to conduct established information operations.

(2) Adverse effects on the Army's image such as Web page defacements.

(3) Access or compromise of classified or sensitive information (for example, soldier identification information (SSN), medical condition or status, patient-client or attorney-client privilege).

(4) Compromise originating from a foreign source.

(5) Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (for example, publicly accessible waterways navigational safety information from the USACE).

7-2. Reporting Responsibilities.

a. An individual who suspects or observes an unusual or obvious incident or occurrence will cease all activities and notify his or her SA/NA, IASO, or IAM immediately.

**Adjutant General's Department
Headquarters, Kansas National Guard
Topeka, Kansas 66611-1287
15 JUNE 2005**

JFHQKS SOP 25-2

b. If the SA/NA, IASO, or IAM is not available, the individual will contact his or her supervisory chain.

**Annex A - APPOINTMENT OF INFORMATION ASSURANCE SECURITY OFFICER
(IASO)**

APPROPRIATE UNIT LETTERHEAD

OFFICE SYMBOL (25-2)

DATE

MEMORANDUM FOR (Individual's Name, Rank, Unit and Address)

SUBJECT: Appointment of Additional Duties

1. Effective _____, (Individual's name)(rank), (unit or Section Address), is appointed the following additional duty:

IASO for the _____ (Directorate/Division Staff/BDE/BN Designation)

2. Purpose. Manage the information management program and advise the Commander/Director on establishing the command priorities for information management. Serve as the interface between the functional user/unit and the J6 for all microcomputer/data communications activities.

3. Period. Indefinite.

4. Special Instructions. Will perform those duties and functions outlined in Army Regulation 25-2.

5. Authority. AR 25-2

(SIGNATURE BLOCK)
(BDE/BN CDR or DIR STAFF)

CF:
Individual
Unit
USPFO
J6
201 File
OPF Tech Pers

**Annex B - THE ADJUTANT GENERAL'S DEPARTMENT
INFORMATION TECHNOLOGY USAGE POLICY/AGREEMENT**

NOTICE AND CONSENT: I _____, understand that the use of any Government Computer or Telephone System constitutes my consent to monitoring of my use of the KSARNG network and systems. I will use this technology responsibly. The contents and communications of this information system, including electronic mail (E-Mail) and Internet access, may be monitored for appropriate use. I understand that there is NO expectation of privacy in using Government computers or resources. I understand that inappropriate use may result in disciplinary action up to and including termination of employment.

PURCHASE AND ACQUISITION: I understand that the Director of Information Management (AGKS-J6) will review all purchase requests and acquisition of telephone, fax, computer equipment, peripherals and software for the Kansas Army National Guard in order to meet user, security and network requirements. All activities, directors, units or training facilities must coordinate with AGKS-J6 through appropriate channels for purchase of telephone, fax, computer systems, or software and the use of personal software (e.g., use of AOL on a Government notebook computer). Violations of this policy may result in disciplinary actions.

TELEPHONE/COMPUTER USE POLICY: I understand that:
Government provided hardware and software are for conducting official government business. Leaders and supervisors may authorize personnel to use government resources to further professional and technical knowledge if it is determined to be in the best interest of the government.

I am accountable and responsible for any transmission I generate, forward, copy or distribute.

Electronic communications are not confidential.

Use of electronic communications such as telephone, fax, E-Mail and the Internet are subject to official agency monitoring and misuse may result in disciplinary action or criminal prosecution.

It is my responsibility to maintain and update AntiVirus software on all computers I am responsible for.

It is my responsibility to maintain an Army Knowledge Online (AKO) account (www.us.army.mil) (military network only)

It is my responsibility to comply with software licensing agreements.

The following activities involving the use of government computers, hardware, software or network systems are specifically prohibited:

Storing, processing, caching, displaying, sending or transmitting language or material that is derogatory, discriminatory, offensive or politically extreme (e.g., hate or racist literature or symbols, information that is derogatory about elected government officials), obscene (child pornography, pornography, sexually explicit) or sexual harassing material.

Storing or processing copyrighted material unless approved in writing by the author or publisher.

Activities for personal or commercial financial gain (e.g., sale of commercial or private property).

Participating in "chat lines" or open forum discussions, unless for official purposes or approved by the Public Affairs Officer at the Adjutant General's Department.

Installing and using any chat software such as AOL IM, Yahoo IM, ICQ.

Installing and using any commercial ISP software on government computers (e.g., AOL, Compuserve).

Using another person's account or identity without appropriate authorization or permission.

Viewing, changing, damaging, deleting or blocking access to another user's files or communications without appropriate authorization or permission.

Attempting to circumvent or defeat security or auditing systems (such as for legitimate system testing or security research) without prior authorization or permission from the Director of Information Management

Installing, copying, storing or using unauthorized software.

Permitting an unauthorized individual access to a government owned, leased or operated system.

Modifying or altering the network operating system or system configuration without first obtaining permission from the Director of Information Management.

Processing classified information on any system not accredited for the necessary classification level.

Prior to individual being granted access to a government network or system, they will sign a statement acknowledging that they have read and understand the provisions of this policy. Each individual's immediate supervisor is responsible to ensure that this occurs prior to system access.

I have read and understand this policy. I understand all information including personal information placed on or sent over the KS-ARNG network may be monitored. I will acknowledge completion with AGKS-J6 prior to receiving passwords.

(Signature of User)

(Date)

Supervisors/Commanders will maintain this signed document in an appropriate filing system (supervisory personnel file, three ring binder, field 201 file, etc.). This completed agreement is subject to inspection.

Annex C - INCIDENT RESPONSE FORM

To be submitted to the IAM through the IASO

Type of Incident _____
Theft, compromise, Virus, malicious code (spyware), social engineering, policy violation, etc....

Name of Target _____ Number of Target _____
Computer name, Person's name, Policy/Regulation violated Phone/IP address

Type of target _____
Person, printer, router, phone, policy, etc....

Operating system of Target _____
Windows XP, Server 2003, Linux, etc...

System Functionality (describe in detail) _____
Mail server, DBIW web server, etc...

Date of incident _____ Time of incident _____

User of target _____ Phone _____ E-mail _____

IASO for target _____ Phone _____ E-mail _____

Unit of target _____ address _____

Perpetrator information _____

Narrative of circumstances _____

**Adjutant General's Department
Headquarters, Kansas National Guard
Topeka, Kansas 66611-1287
15 JUNE 2005**

JFHQKS SOP 25-2

Annex D - NGB ACQUISITION POLICY

DEPARTMENTS OF THE ARMY AND AIRFORCE
NATIONAL GUARD BUREAU
111 SOUTH GEORGE MASON DRIVE
ARLINGTON, VA 55504-1382

NGB-AIP-PP

23 June 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Review Requirement for all Acquisitions of Information Technology (IT) Equipment and software Acquisitions

1. This document states the Army National Guard (ARNG) policy for review of all acquisitions of IT and IT Resources.

The requirements for Senior IT Staff review all purchases of IT of IT Resources set forth in this document apply to the ARNG. Setting and maintaining these standards serves to provide a minimum level of coordination and serves to assist in ensuring interoperability, integrability and compliance with the Joint Technical Architecture—Army.

All purchases and acquisitions of IT or IT Resources must be reviewed by a Senior IT Staff Member of the State, Territory, or District of Columbia. All acquisitions of IT or IT resources for USP&FO operations must be reviewed by the DPM as a minimum. All other IT acquisitions within the States must be reviewed by the J6s/DOIMs.

The IT and IT Resources are identified in Army Regulation AR 25-1, Army Information Management, 31 May 2002. Paragraph 1-5(a) explains the use of the term Information Resources. Paragraph 1-5(b) of the same regulation explains the use of the term IT.

The point of contact for this policy is Mr. Lawrence Ford, 703-607-7686 e-mail lawrence.ford.ngb.army.mil

\\Original signed//
BOBBY L. MCKINNON
Colonel, General Staff
G6, Army National Guard

Distribution:
NGB-IG
NGB-PL
NGB-AIS
Each State Cofs
Each State IG
Each State USP&FO
Each State DOIMS/J6/J6
Each State DPM
Each State Public Affair

Annex E – Sample Accreditation Letter



DEPARTMENTS OF THE ARMY AND THE AIR FORCE
Joint Forces Headquarters Land Component
2800 SOUTHWEST TOPEKA BOULEVARD
TOPEKA KANSAS 66611-1287

AGKS-DSCIM-CERT

(DATE)

MEMORANDUM FOR RECORD

SUBJECT: Accreditation of Automated Information System (AIS).

1. The following information covers the AIS .
 - a. Type XXXXXXXX
 - b. Make XXXXXXXX
 - c. Model XXXXXXXX
 - d. Serial Number XXXXXXXX
 - e. NIC MAC address XXXXXXXX
 - f. Hostname XXXXXXXX
2. The AIS is accredited to process (CLASSIFICATION) AND BELOW.
3. This accreditation is valid for one year, or if the basic configuration is changed by adding or removing hardware/software.
4. This letter of accreditation must accompany covered AIS at all times.

SIGNATURE
Rank, Br
Information Assurance Manager

Annex F – IASO Binder Tabs

Information Assurance Security Binder		
Table of Contents		
A		Appointment letters
B		User Training Certificates/Signed Policy letters
C		List of Assets
D		List of Users
E		Computer accreditation letters
F		Incidents
G		Copy of Last inspection
H		Copy of inspections over last three years
I		X.509 certificates

Annex G – Inspection Checklist

Information Assurance Checklist			
1	Does the system not display the last user?	Yes	No
	Ref: KS-SOP-25-2		
	Data: [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system] "dontdisplaylastusername"=dword:00000001		
2	Does the system have an antivirus definition of not more than a week old?	Yes	No
	Ref: AR 25-2 P. 4-5 n		
	Data: Click on shield & ensure server is ngksc3-20315nav and date is less than 1 week		
3	Does the system have the SMS client installed?	Yes	No
	Ref: KS-SOP-25-2		
	Data: control panel, SMS ensure sitecode is KS0		
4	Does the system have a designated SUS server?	Yes	No
	Ref: KS-SOP-25-2		
	Data: [HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate] WUServer="http://ks-20315-sus"		
5	Do all users have a signed IT usage agreement on file with the IASO?	Yes	No
	Ref: AR 25-2 P. 4-5 r		
	Data: Will be in IASO Binder		
6	Have all users taken and passed the user security training within the last year?	Yes	No
	Ref: AR 25-2 P. 3-3 c. (1) (a)		
	Data: Will be in IASO Binder		
7	Have all power users taken the IASO course?	Yes	No
	Ref: KS SOP-25-2		
	Data: Will be in IASO Binder		
8	Have all administrators taken the System Administrators/Network Managers Course?	Yes	No
	Ref: AR 25-2 P. 3-3 a.		
	Data: Will be in IASO Binder		
9	Does the system belong to the domain?	Yes	No
	Ref: KS SOP-25-2		
	Data: right-click on my computer, properties, computer name		
10	Is a password protected screen saver activated after 10 minutes of inactivity?	Yes	No
	Ref: AR 25-2 P. 3-3 c. (1) (l)		
	Data: Right click on desktop, properties, screen saver		
11	Does the system have a warning banner and last name disabled?	Yes	No
	Ref: AR 25-2 P. 4-5 l (2)		
	Data: [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] PowerdownAfterShutdown="1" DontDisplayLastUserName="0" LegalNoticeCaption="ATTENTION"		