



REPLY TO  
ATTENTION OF

**DEPARTMENT OF THE ARMY**  
**HEADQUARTERS & HEADQUARTERS BATTALION**  
**2ND INFANTRY DIVISION**  
**UNIT # 15041**  
**APO AP 96258-5110**

**23 NOV. 2015.**

EAID-CG

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter # 6-1, Information Management Officer/Information Assurance Officer

1. References:

- a. 2ID Command Policy Letter #6-1, Information Assurance, dtd 28 February 2012 (Superseded).
- b. DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management, dtd 23 April 2007
- c. DoD 8570.01-M, Information Assurance Workforce Improvement Program, incorporating change 3, dtd 24 January 2012.
- d. AR 25-1, Army Knowledge Management and Information Technology, dtd 4 December 2008.
- e. AR 25-2, Information Assurance, (Rapid Action Revision), dtd 23 March 2009.
- f. Army in Korea Supplement to AR 25-1, Army Knowledge Management and Information Technology, dtd 2 July 2009.
- g. Army in Korea Supplement to AR 25-2, Army Information Assurance, dtd 12 July 2006.
- h. 2ID Command Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures, dtd 10 August 2012.
- i. 2ID Information Assurance Incident Response Plan, dtd 7 January 2013.
- j. Army in Korea UNCLASSIFIED / CLASSIFIED LandWarNet (AKULWN / AKCLWN) Account Management Policy, version 3.0.0, dtd 19 November 2012.

2. Applicability. This policy applies to all personnel assigned, attached, or under the operational control of 2d Infantry Division (2ID), including Department of Defense (DoD) and Local National (LN) civilian employees, invited contractors, technical representatives, and all Family Members.

EAID-CG

SUBJECT: Policy Letter #6-1, Information Assurance

3. Policy. Information Assurance (IA) is a commander's program at all levels to implement and enforce. All leaders are charged with ensuring compliance with this policy letter and will remain cognizant at all times of their unit's IA posture and take appropriate actions to mitigate risks to information and Information Systems (IS) under their control. All personnel will adhere to the specific policy guidance below:

a. Cyber Environment Posture. Enclosure 1 details network and IS compliance and restrictions.

b. Systems Access. Enclosure 2 lists account processing, usage, and general user training requirements.

c. Prohibited Activities. Enclosure 3 stipulates usage prohibitions.

d. Incident Management. All suspected information assurance violations will be reported through the organization Information Management Officer (IMO)/Information Assurance Manager (IAM)/Information Assurance Support Officer (IASO)/System Administrator (SA) to the 2ID IAM. See Section 4 of the 2ID IA Incident Response Plan for the Division Incident Response Checklist. Incident s involving Unauthorized Disclosure of Classified Information will be processed IAW 2 ID Policy Letter #6-2.

4. Violations and Corrective Measures. Due to the interconnected nature of DoD networks, a vulnerability introduced on one 2ID system or network greatly increases operational risk throughout DoD and is unacceptable. Commanders will take appropriate actions to investigate, retrain, or punish personnel suspected of engaging in prohibited computer-network activities and take protective measures to implement controls and prevent unauthorized activities. The security of 2ID systems and networks is everyone's responsibility. Enclosure 4 details corrective and remedial measures.

5. IA Workforce. All leaders in the grade O-5 or higher will ensure appointment and certification of IA workforce personnel IAW Enclosure 5. Positions listed in Enclosure 5 are permanent and replacements must be appointed prior to incumbents departing the Division. Report all appointments to the 2ID IAM.

6. Proponent for this policy letter is 2ID C6, 315-732-6081. Point of Contact is the C6 IA Section, [usarmy.redcloud.2-id.list.g6-ia@mail.mil](mailto:usarmy.redcloud.2-id.list.g6-ia@mail.mil) , 315-732-6459/8841/8808/7337.

EAID-CG

SUBJECT: Policy Letter #6-1, Information Assurance



THEODORE D. MARTIN  
Major General US Army  
Commanding

5 Encls

1. Cyber Environment Posture
2. System Access
3. Prohibited Activities
4. Remediation and Corrective Measures
5. IA Workforce

DISTRIBUTION

A

Enclosure 1 (Cyber Environment Posture) To 2ID Policy Letter #6-1, Information Assurance

1. All automation, computing, network, and Portable Electronic Devices (PEDs) connected to the network or stand alone will comply with Department of the Army published Certification and Accreditation (C&A) and Information Assurance Vulnerability Management (IAVM) directives and network security policies.
2. All computers, laptops, PEDs, and media will be Data-At-Rest (DAR) compliant, will be labeled with the appropriate level of classification, and will be government furnished equipment. Virtual Private Network (VPN) accounts require a DAR compliance check of portable electronic devices before use outside of the ordinary office environment and, upon return, will be scanned for vulnerabilities and remediated prior to normal operation.
3. All removable computer-system media must be government-owned and properly marked controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know. All removable media will be scanned for viruses before use on Government systems.
4. Sensitive Information (SI)/ Personally Identifiable Information (PII). PII is any information about an individual that is private or intimate to the individual and as distinguishing from information related solely to the individual's official functions or public life. The information includes, but is not limited to, any personal information which is linked or linkable to an individual, such as education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual's identity. Examples include social security numbers, date and place of birth, mother's maiden name, and electronic medical records. SI/PII requires special handling and will be protected as follows:
  - a. SI/PII will be encrypted when contained within an e-mail or removed from a government facility, and will be DAR compliant if required to be stored locally.
  - b. SI/PII not required for immediate mission processing will be removed from the local IS.
  - c. PII will not be posted to a Sharepoint Portal in any form under any circumstances.
5. Commanders will ensure compliances with enterprise C&A policy.
  - a. AKULWN/AKCLWN Network Change Proposals (NCP) and Joint Requirements Documentation or proposals will be submitted through the C6 IA section (to the proponent agency, Network Enterprise Center (NEC) NLT 90 days prior to Command Communications Service Designator (CCSD) or Tenant Security Plan (TSP) expiration.
  - b. Tracking documentation such as Hardware/Software (HWSW) Lists, connectivity charts, and physical diagrams will be continuously updated and maintained at all levels.
6. Administrators at all levels will take active measures to mitigate vulnerabilities and implement controls in order to ensure the security of 2ID IS. Systems identified as non-compliant, improperly configured, compromised, or involved in prohibited activity will be immediately removed from the network and quarantined until remediation is complete or the system is reloaded to baseline standards.

## Enclosure 2 (System Access) To 2ID Policy Letter #6-1, Information Assurance

1. Prior to accessing any 2ID owned system, all users must meet minimum security requirements IAW AR 25-2, Section V.
2. Prior to accessing any 2ID owned system, all users (including transients, DoD visitors, temporary or seasonal workers, KGS or LN Civilians, KSCs, KATUSAs, Contractors, interns, Volunteers, or users not generally processed for permanent accounts) must read and sign the current Acceptable Use Policy (AUP) Acknowledgement/User's Agreement for the enclave or system they are attempting to access. For access to stand alone or separate Program Managed (PM) systems, users without an Army Training and Certification Tracking System (ATCTS) profile (see 3.a below) will read/sign/and maintain local copy of the Army Standard AUP available at <https://atc.us.army.mil/iaster/docs/aup.pdf>.
3. All personnel requesting general user access to 2ID systems or networks will complete the following items prior to accessing IS or being processed for account creation.
  - a. Register in ATCTS at <https://atc.us.army.mil/iaster/>. Sign into account at least once using CAC.
  - b. Complete and successfully pass, within the last 12 months, DoD directed Army DoD Cyber Awareness Training and exam at <https://ia.signal.army.mil/DoDIAA/>. This training must be completed annually and this automatically updated in ATCTS.
  - c. Read, sign, and upload the current AK Form 25-2, Korea LandWarNet Acceptable use Policy, to their ATCTS profile. AK Form 25-2 is available at [http://8tharmy.korea.army.mil/gl\\_AG/Programs\\_Policy/Publication\\_Records\\_Forms.htm](http://8tharmy.korea.army.mil/gl_AG/Programs_Policy/Publication_Records_Forms.htm).
  - d. Complete a System Authorization Access Request (SAAR), DD Form 2875, and upload to ATCTS profile. The SAAR must be filled out completely and digitally signed by authorized personnel (see para 6). Use the official form, the lockable version of the SAAR, available at <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2875.pdf> or locking version required by the local Area IC, NEC, or proponent agency.
4. All users with authorized access to PII will annually review and sign AK Form 25-2 in conjunction with the completion of DoD Annual IA Refresher training and upload to their ATCTS profile.
5. Privileged Users and IA managers. All privileged level access request will be processed through the G6 IA section, no exceptions. All IA Workforce personnel, including privileged users and technical personnel requiring local administrator privileges will, in addition to the above requirements:
  - a. Complete all DoD and Army training and certification requirements based on assigned IA level and category.
  - b. Read and sign the current 2ID Privileged Access Agreement (PAA) and post to their ATCTS profile.

## Enclosure 2 (System Access) To 2ID Policy Letter #6-1, Information Assurance

- c. Post position appointment orders to ATCTS profile.

Notes: See Enclosure 5 for IA Workforce assignments and certification requirements.

6. Account Processing Signature Authority. Account requests require validation by authorized personnel via digital signature in blocks 21 and 22 of the SAAR. To ensure proper separation of duties, one person may not sign in multiple boxes of the SAAR. In the absence of assigned personnel at lower levels, SAARs will be elevated to the next higher level for validation (i.e., from BN S6 to BDE S6 or DIV IA).

- a. Only those personnel properly assigned on orders as a System Administrator may sign in block 21 of the SAAR.

- b. Only those personnel properly assigned on orders as an IAM, IAO, or IASO may sign in block 22 of the SAAR.

7. Access to 2ID resources is a revocable privilege and all access is assigned on an individual basis and is non-transferable. Users are accountable for access and must maintain control of login credentials, CACs, and tokens at all times. Compromised access credentials or lost tokens must be immediately reported to the organization SA, IASO/IOA or IAM.

8. All user privileges will be terminated and accounts deleted upon departure from the Division, Permanent Change of Station (PCS) or Expiration of Term of Service (ETS). The activity / section creating an account is directly responsible for tracking, disabling, and removing accounts for departing personnel. ATCTS managers will ensure user profiles are inactivated for departing personnel.

## Enclosure 3 (Prohibited Activities) To 2ID Policy Letter #6-1, Information Assurance

1. No external computing, wireless, or storage devices are allowed to be connected to 2ID information systems (IS) or networks, including all types of USB devices, flash media, SD/microSD, eSATA, readers, tablets, PEDs, or cell phones if not explicitly approved by the 2ID IAM. Chargeable devices (cell phones, tablets, readers, PEDs, etc.) will not be attached to USB ports for charging. No personally owned electronic, computer, network, or storage devices are allowed to be connected to 2ID information systems or networks regardless of situation. The only removable media authorized on a 2ID IS are DVDs/CDs.
2. No externally sourced software (including executable files not requiring installation), Peer-to-Peer downloads, Instant Messaging, or games are allowed on government information systems if not explicitly approved by the 2ID IAM.
3. No authorized installation or removal of programs, disabling of security configurations or audit logs, altering system configurations, straining, testing, circumventing, or bypassing security mechanisms to include enabling the use of thumb drives or external media unless explicitly permitted by the 2ID IAM.
4. Prohibited use of 2ID IS and networks also includes:
  - a. Transferring account credentials or login privileges to another user. Users will not allow, under any circumstances, another individual to 'borrow' their login, CAC, or token to access 2ID systems.
  - b. Use of IS that adversely reflects on DoD, the Army, or 2ID such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images; chain email messages; unofficial advertising, soliciting, or selling via email; and other uses that are incompatible with public service.
  - c. Use of IS for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DoD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or public laws. This includes, but is not limited to: violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.
  - d. Political traffic to include transmissions that advocate the election of particular candidates for public office.
  - e. Theft or other abuse of computing facilities or services. Such prohibitions apply to electronic mail service and include, but are not limited to unauthorized entry; use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities.
  - f. Use of a 2ID IS for purposes that could directly or indirectly cause congestion, delay or disruption to enclave services or computing facilities or cause unwarranted or unsolicited interference with another person's access to or use of computing resources or facilities. Such activities include the use of IS to:

Enclosure 3 (Prohibited Activities) To 2ID Policy Letter #6-1, Information Assurance

- (1) Create, download, store, copy, transmit, or broadcast chain letters.
- (2) "Spam" to exploit list serves or similar broadcast systems for purposes beyond their intended scope, to amplify the widespread distribution of unsolicited e-mail.
- (3) Send an email bomb (consisting of huge volumes of email), or to re-send the same email message repeatedly to one or more recipients, to interfere with the recipient's use of email.
- (4) Broadcast unsubstantiated virus warnings from sources other than system administrators.
- (5) Broadcast unofficial e-mail messages to large groups of e-mail users.

5. Privileged Level Prohibited Use. Privileged level users are appointed, trained, and trusted to follow/enforce policy and ensure systems and networks remain secure. Privileged level violations are unacceptable and are a breach of trust between the individual, 2ID, and the Army. Privileged level users who do not follow/enforce information assurance policies are negligent in their duties, introduce vulnerabilities, and place our mission at unnecessary risk. Privileged level violations include, but are not limited to:

- a. Disclosing or transferring administrative credentials or tokens to unauthorized personnel.
- b. Providing system access to unauthorized individuals or providing access to personnel who have no completed access requirements detailed in Enclosure 2.
- c. Installing any unauthorized hardware, software, backdoors, or malicious code.
- d. Subverting data protection schemes to gain access to, share, or elevate permissions or privileges to unauthorized data or systems.
- e. Failing to report any indication of computer-network intrusion, unexplained degradation, or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate IA Workforce.
- f. When vulnerabilities have been identified, failing to implement controls or remediation procedures to ensure the security of systems under their purview.
- g. Disabling CAC or token enforcement settings.

Enclosure 4 (Remediation & Corrective Measures) To 2ID Policy Letter #6-1, Information Assurance

a. Failure to follow any of the procedures of this policy letter, abide by its prohibitions, or violating DoD or Army regulations will result immediate suspension of network access and privileges.

c. These provisions may be punished as follows.

(1) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; suspension access to IS or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; and or dismissal from employment. Sanctions for civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Only civilian managers or military officials who have authority to impose the specific sanction proposed may award sanctions.

(2) Sanctions for military personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; and loss of suspension of access to IS or networks and classified material and programs. Sanctions for military personnel may also include any administrative measures authorized by service directives and any administrative measures of non-judicial or judicial punishments authorized by the Uniform Code of Military Justice (UCMJ).

b. Regardless of severity, the following must be completed to reactivate a user account.

(1) First Offense – Memorandum signed by the first commander/director in the chain of command that is in the grade of O-5 or GS-14 equivalent, retake the cybersecurity awareness training, and re-sign the Acceptable User Policy AUP. The O-5 memorandum must state what actions and corrective training was completed to prevent reoccurrence. After a 7 day suspension, the account may be reactivated once the signed memorandum has been received and accepted by the 2ID IAM.

(2) Second Offense – Memorandum signed by the first commander/director in the chain of command that is in the grade of O-6, GS-15 equivalent, retake the cybersecurity awareness training, and re-sign the Acceptable User Police AUP. The memorandum must state what actions and what corrective training was completed to prevent reoccurrence. After a 30 day suspension, the account may be reactivated once the signed memorandum has been received and accepted by the 2ID IAM.

(3) Third offense – A third offense will result in user's permanent loss of network access.

c. Privileged level violations. Commanders will initiate an investigation involving any report of privileged level violation and ensure privileged level user access and access to classified information is suspended immediately pending investigation results. Where violations of Army policy and/or negligence or misconduct are founded, privileged level access will not be reinstated to the individual and an incident report will be opened in the Joint Personnel Adjudication System (JPAS) for adjudication and tracking purposes.

Enclosure 5 (IA Workforce) To 2ID Policy Letter #6-1, Information Assurance

1. The IA workforce focuses on the operation and management of IA capabilities for DoD systems and networks. IA ensures that adequate security measures and established IA policies, controls, and procedures are applied to all IS and networks. The IA workforce includes all privileged users, specialty positions, and IA managers who perform any of the functions described in DoD 8570.07-M, across all occupational specialties, or whether the duty is performed full-time or part-time as an additional/embedded duty.
2. DoD 8570.01-M requires all DoD Information Assurance (IA) personnel to obtain and maintain a commercial certification commensurate with their appointed IA technical or management levels. Army IA training and certification guidance requires that 100% of filled IA positions are held by IA trained and certified personnel. Compliance levels are reported to HQDA on a semi-annual basis through ATCTS.
3. All 2ID IA Workforce personnel will meet AR 25-2 security requirements; will be certified IAW DoD 8570.01-M for baseline and Computing Environment (CE) requirements; and will process for privileged access based on level of assignment. Levels are defined as: Information Assurance Management, level I/II/III (IAM-I/II/III) or Information Assurance Technical, level I/II/III (IAT-I/II/III). Unless otherwise specified or assigned, information assurance support officers (IASO) and Information Management Officers (IMO) do not have baseline or CE certification requirements.
4. Mandatory minimum required IA Workforce position in 2ID and the unit and organization levels at which the positions must exist and be filled by qualified personnel are specified below. Individuals filling these positions must be appointed on orders and appointments reported to the 2ID IAM.

a. Brigades:

(1) Appoint the Brigade Information Assurance Manager (IAM). This position is dual appointed as IAM/SA, requires Organizational Administrator (OA) privileges and IAM-II / IAT-II certifications.

(2) Appoint the Brigade Information Assurance Officer (IAO). This position is dual appointed as IAO/SA, requires Organizational Administrator (OA) privileges and IAM-I / IAT-II certifications.

(3) Appoint the Brigade Information Management Officer (IMO). This position is dual appointed as IMO/SA, requires Organizational Administrator (OA) privileges and IAM-I / IAT-II certifications.

(4) Appoint the Brigade System Administrator (SA). This position requires Organizational Administrator (OA) privileges and IAT-II certification.

b. Battalions:

Enclosure 5 (IA Workforce) To 2ID Policy Letter #6-1, Information Assurance

(1) Appoint the Battalion Information Assurance Officer (IAO). This position is dual appointed as IAO/SA, requires Account Operator (AO) privileges and IAM-I / IAT-II certifications. Personnel may be assigned as both S6 and IAO.

(2) Appoint the Battalion Information Management Officer (IMO). This position is dual appointed as IAO/SA, requires Account Operator (AO) privileges and IAM-I / IAT-II certifications. Personnel may be assigned as both S6 and IAO.

(3) Appoint the Battalion System Administrator (SA). This position requires Account Operator (AO) privileges and IAT-II certification.

c. Staff Sections/Offices headed by Lieutenant Colonel or equivalent:

(1) Appoint the Information Assurance Support Officer (IASO). This position does not require commercial certification. Personnel may be dual appointed as IASO/IMO.

(2) Appoint the Information Management Officer (IMO) This position does not require commercial certification. Personnel may be dual appointed as IASO/IMO.

Note: Staff sections with multiple O-5 level offices must appoint an IASO for each office in addition to the IASO appointed for the primary staff section.

d. 2ID C6:

(1) Assign the Division Information Assurance Manager (IAM). This position is dual appointed as IAM/SA, requires Organizational Administrator (OA) privileges and IAM-III / IAT-II certifications.

(2) Appoint the Division Information Assurance Officer (IAO). This position is dual appointed as IAM/SA, requires Organizational Administrator (OA) privileges and IAM-II / IAT II certifications.

(3) Appoint the C6 Information Assurance Officer (IAO). This position is dual appointed as IAM/SA, requires Organizational Administrator (OA) privileges and IAM-I / IAT II certifications.

(4) Appoint two personnel as Division System Administrators (SA). These positions require Organizational Administrator (OA) privileges and IAT-II certifications.

e. Other IA Workforce assignments:

(1) Personnel assigned as managers in ATCTS (S6s, IMOs, Help-Desk Technicians, etc.) will be appointed on orders detailing the IA function performed. Orders will contain proper IA regulation citations, for example – Purpose: To perform IA functions and duties per AR 25-2 paragraph 3 and DoD 8570.01M.

Enclosure 5 (IA Workforce) To 2ID Policy Letter #6-1, Information Assurance

(2) Local Administrator Requirements. Technical personnel, help-desk technicians, and IMO's requiring local administrator access to 2ID systems will meet IAT-I certification requirements and process requests through C6 IA for privileged access.

(3) Commanders, Managers, Directors may appoint additional IA Workforce personnel as required to enforce IA policy within the Division.

(4) Designated Approving Authority (DAA), Designated Approving Authority Representative (DAAR), Certification Authority (CA), and Agent of the Certification Authority (ACA) positions are reserved within the Division and will be coordinated through the 2ID IAM, the C6 and the Command Group if required.