



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, 15TH REGIMENTAL SIGNAL BRIGADE
606 BARNES AVENUE
FORT GORDON, GEORGIA 30905-5729

ATZH-TB

20 January 2015

MEMORANDUM FOR All Assigned and Attached Military and Civilian Personnel

SUBJECT: Policy Letter #20: Use of Automation Information Systems

1. References:

- a. ALARACT 050/2009, Personally Identifiable Information (PII) Incident Reporting and Notification Procedures, 26 February 2009.
- b. ALARACT 293/2007, Implementation of Standard DOD IA Awareness Training, 26 December 2007.
- c. AR 25-1, Army Information Technology, 25 June 2013.
- d. AR 25-2, Information Assurance, 24 October 2007 (RAR 001, 23 March 2009).
- e. AR 25-400-2, The Army Records Information Management System (ARIMS), 2 October 2007.
- f. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- g. DOD Directive 8570.01-M, Information Assurance Workforce improvement Program, 19 December 2005 (incorporating change 3, 24 January 2012).
- h. Memorandum IA BBP, 06-EC-0-0008: Data at Rest (DAR) Protection, 18 October 2006.

2. This policy applies to all Brigade personnel. Brigade personnel are defined as permanent party military (includes Fort Meade and sister service detachments), Civilian Employees, contractors, IET and Non-IET Soldiers, as well as visitors and guests while in our care.

3. Purpose. This memorandum establishes Command policy regarding End-User access to and the safe operations of all Government owned Automated Information Systems (AIS). Information Systems (IS) are defined as, but not limited to, computers, processors, devices, or environments (operating in prototype, test bed, stand-alone, integrated, embedded, or networked configuration) that store, process, access, or transmit data, including unclassified, sensitive (formerly known as sensitive but unclassified (SBU)), and classified data, with or without handling codes and/or caveats. This policy further extends authority over ISs that are used for teleworking, telecommuting, or similar initiatives; contractor owned or operated ISs; all ISs obtained with non-appropriated funds; automated tactical systems (ATs); distributed computing environments (DCEs); and any Commercial off the Shelf (COTS) devices purchased for the intent of providing a classroom training environment.

4. Information Systems Access Requirements.

a. Authorized User. A trained and aware user is the first and most vital line of defense in defending our networks. The following minimum training is required by all users prior to accessing any ISs as defined in this policy. Users are required to complete Personally Identifiable Information (PII) and Portable Electronic Device training modules using the Wide Network Security Focus (WNSF) versions found at the following web sites:

(1) DoD Cyber Awareness Challenge Training, located at <https://ia.signal.army.mil> .

(2) WNSF – PII Training, located at <https://iatraining.us.army.mil> .

(3) Fort Gordon DAR Training, located at <https://ia.signal.army.mil>

(4) Acceptable Use Policy. A local copy of the most current version as published by the Fort Gordon NEC must be signed in all applicable blocks by each user and updated annually. Digital signatures via Common Access Card (CAC) are required and the form must be uploaded manually to each users ATCTS account prior to access being granted.

(5) WNSF – Portable Electronic Devices and Removable Storage Media v2.0, located at <https://iatraining.us.army.mil>, this training is mandatory only for users of Government provided smart phones and must be updated annually.

b. Privileged User. A privileged user is defined as any user that is granted elevated privileges on any information system at the minimum level required to perform their technical support function as outlined in the DoD Directive 8570.01-M paragraph C3.2. All privileged level users are required to complete all of the training required above for authorized users as well as the minimum training and certification levels outlined in DoD 8570.01 according to the IAT/IAM level they are assigned.

ATZH-TB

SUBJECT: Policy Letter # 20: Use of Automation Information Systems (AIS)

(1) Information Assurance Work Force (IAWF) will maintain two access credentials, one for their authorized access (general user, CAC) and a second credential for their elevated privilege level, Alternate Smart Card Login (ASCL, CAC).

(2) Elevated privileges in the form of administrative usernames and passwords will be issued for information systems that are not CAC enabled within the Fort Gordon Campus Area Network (FGCAN) only after all training and certifications required are authenticated by the Brigade Information Systems Branch.

c. Web Site Administrator/Web Content Manager. Personnel assigned as either Web Site Administrators or Web Content Managers are required to maintain all public and private web sites within the organization including ensuring that all content meets current security policies regarding PII and OPSEC.

(1) Web Site Administrators are defined as those personnel granted access to the core server components of the web server used to host web pages as well as administrative access to the web site content and structure. At a minimum, these personnel will be assigned the role of IAT Level I in addition to completing the Certified Internet Web Professional (CIW) Foundations Certification.

(2) Web Content Managers are defined as those personnel granted elevated privileges of the content contained within organizational web sites, not the structure or core components of the servers. Content Managers are not required to hold any IAT Level certifications, but must complete the following training prior to being approved for appointment orders: Social Media and Operations Security, located at <https://ia.signal.army.mil>.

5. Personally Identifiable Information Safe Storage and Handling.

a. PII is defined as any information about an individual which can be used to distinguish or trace an individual's identity such as, but not limited to, name, social security number, date and place of birth, mother's maiden name, and biometric records. This information is extended to any unique identification given to a user on either a permanent basis or temporary basis such as, but not limited to, employee ID numbers and student ID numbers used to trace records for identification purposes.

b. PII storage on computer systems. The storage of records or digital files that contain records that are considered PII must be handled according to the safe practices outlined within AR 380-5 and AR 25-2.

(1) Stored files on any information system must be encrypted using the current approved version of Data-At-Rest desktop encryption software. Files that are stored on portable devices must be encrypted using a total disk encryption software system approved under the US Army Gold Master program.

ATZH-TB

SUBJECT: Policy Letter # 20: Use of Automation Information Systems (AIS)

(2) Files that are uploaded to shared drives and TKE provided share point web sites must be stored in folders that are secured through access control lists. Access to the files must be closely monitored and restricted to only those that have an inherent need to know the information for current operational duties. Group folders are not authorized storage containers for PII files unless access to the group area is restricted on a need to know basis.

c. PII transfer of files through electronic means. Files that contain PII may be transferred through electronic mail (e-mail) programs as long as they are digitally signed using an approved CAC certificate and are digitally encrypted throughout the transfer. Files with PII are never authorized to be transferred outside a government server email domain (i.e. .mil) under any circumstances and are not authorized for use, storage, or viewing on any personally owned information system or computer device.

d. PII Incident Reporting Requirements. Loss of personal information can have vastly detrimental effects on both National Security as well as individual's personal life. An incident occurs when it is suspected or confirmed that PII is lost, stolen, or otherwise available to individuals without a duty related official need to know. This includes but is not limited to sending unencrypted files that contain PII to an information system that is outside the government server (from .mil to .com email address). Incident procedures should be strictly followed according to ALARACT 050/2009 concerning all confirmed or suspected breaches in PII security.

(1) Any incidents that involve either suspected or confirmed breach or loss in PII must be reported to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery of the breach or loss.

(2) This report is followed by a more detailed report being filed through the Brigade Information Systems Branch and local Chain of Command channels.

e. Unapproved PII gathering applications. Applications or programs to include, but not limited to, databases that are specifically designed to gather information about an individual and used for identification purposes must be handled with special care. Units are not authorized to create their own version of these programs or databases unless they are approved for use on government systems through the DISA Certificate of Net-worthiness section. Programs such as these that are not handled appropriately can cause detrimental and sometimes catastrophic breaches in security if they are not maintained appropriately.

(1) Programs with the sole purpose or intent to gather and store records of personal information about our workforce including students must meet all current applicable policies and safeguards set forth in all referenced Regulations and Policies.

ATZH-TB

SUBJECT: Policy Letter # 20: Use of Automation Information Systems (AIS)

(2) These programs must be stored on a government system that is maintained current with all applicable security patches and governed by the approved Group Policy rules applied to government systems. Programs at a minimum will provide built in encryption for all data stored while at rest and CAC authenticated user access to the program records while in use.

6. Compliance scanning of all automated information systems. All information systems in use by government personnel, and their contractors must be scanned for compliance of all applicable security regulations and policies. Information Systems that are not connected to the FTCAN must be manually inspected periodically to ensure compliance. This scanning will be conducted at a minimum (quarterly) unless otherwise mandated by Program Manager (PM) dictated guidelines. Computer systems will be accessed only by authorized means according to current rules set forth in AR 25-1 and AR 25-2 unless a specific mission related exception to the policy is approved in writing and authorized by the FTCAN Designated Accreditation Authority (DAA). This includes all Information Systems that must utilize legacy Operating Systems (OS) and those that are not able to use CAC authentication services provided by the installation RADIUS systems.

a. Information Systems that are designated as approved for Username/Password local login (i.e. Student computers in the training environment) must meet all other policies and applicable standards concerning the safe use of passwords in the government IT environment.

b. Passwords will be changed on a rotational basis no less than quarterly and records of the compliance will be reported to the Brigade Information Systems Branch through IAWF personnel.

c. Usernames will be created with the concept of "least privilege necessary" in order to meet the intent of the training. Administrator access to government systems are restricted to those personnel that meet the requirements outlined in DoD 8570.01 and designated in writing as IAT Level I, II, III certified personnel.

7. For more information about AIS, contact the Brigade Information Systems Branch at (706) 791-5512.


MARCUS A. REESE
COL, SC
Commanding