TEXAS MILITARY DEPARTMENT
POST OFFICE BOX 5218
AUSTIN, TX 78763-5218
(512) 782-5001

NGTX-JIZ 2 October 2018

MEMORANDUM FOR All Texas Military Department and Texas Army National Guard Personnel

SUBJECT: Information Technology (IT) Acceptable Use Policy (AUP) and User Responsibility Agreement

1. References.

a. Army Regulation 25-2, Information Management, Information Assurance, 24 October 2007

b. Army Regulation 380-5, Department of the Army Information Security Program, Dated 29 September 2000.

c. Army Regulation 380-53, Information Systems Security Monitoring, 23 December 2011.

d. Department of Defense (DoD) Chief Information Officer (CIO) Memorandum, Subject: Policy on Use of DoD Information Systems - Standard Consent Banner and User Agreement, dated 9 May 2008.

2. Purpose. To promulgate policy regarding the authorized uses of IT Resources within or under the control of the Texas Military Department (TMD) to insure that information and computer systems are used responsibly, professionally, ethically and legally.

3. Applicability. This policy is applicable to all elements of The Texas Military Department and any other person who in the course of their duties under the control of the Adjutant General of Texas, and with the approval of the Director of Information Management (DOIM), accesses TMD IT Resources. Violations of this policy may result in disciplinary action which can include administrative punishment and/or criminal prosecution.

4. Background. Multiple Federal entities that have purview in conjunction with DoD, DA, NGB, CIO, and TMD CIO have established guidelines to ensure the effective and efficient use of Federal IT Resources. The policies contained in this memorandum are consistent with those guidelines.

5. Definitions.

a. IT Resources refers to all TMD owned network and communications systems and devices. TMD IT Resources include but are not limited to, host computers, file servers, application servers, mail servers, web servers, communications servers, work stations, thin-client computing platforms, stand-alone computers, laptop computers, Personal Data Assistants (PDA), government issued cell phone devices, tablets, software, video and data files, telecommunications devices (telephones, video teleconferencing, etc.) and all internal and external communications networks that may be accessed directly or indirectly from the TMD computer network. IT Resources refer to both classified and unclassified information processing and include both normal operating environments and emergency communications environments.

b. Users refers to all assigned personnel at TMD, military or civilian, temporary workers, students, contracted employees or any other authorized persons who use TMD's IT Resources.

c. Information Systems Security Manager (ISSM) is responsible for the Information Assurance (IA) program and Cyber Security of an Information System (IS) within the network environment (NE). TMD ISSM performs a variety of security related tasks including the development and implementation of system information security standards and procedures. ISSM ensures that IS are functional and secure within the NE.

d. Classified Information Processing Secure Internet Protocol Routed Network (SIPRNET) is the primary classified Information System for Army Units. SIPRNET is used for information traffic that is classified at a level not to exceed SECRET. It is the only system approved to process collateral information with all appropriate handling instructions for that level of classification.

(1) The SIPRNET provides classified communication to external DoD agencies and other U.S. Government agencies via electronic mail.

(2) The SIPRNET is authorized for SECRET level processing in accordance with accredited SIPRNET ATO.

(3) The classification boundary between SIPRNET and Non-secure Internet Protocol Routed Network (NIPRNET) requires vigilance and attention by all users.

(4) The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

e. Unclassified Information Processing on the NIPRNET, is the primary unclassified Information System for Army Units.

(1) 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, and Terminal Server Access Controller System (TSACS).

(2) NIPRNET is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2 and local automated Information System security management policies.

(3) The NIPRNET and the Internet, for the purpose of this 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, hackers), and internal threats.

f. Emergency Communications are normally utilized during an identified period of response to manmade and natural disasters. Refer to specific emergency communications SOPs for limited adjustments to this AUP.

g. Personally Identifiable Information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII could potentially be exploited to criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts. Examples of PII include but are not limited to Social Security Number (SSN), Date of Birth (DOB), Place of Birth, Mother’s Maiden Name and biometric records.

6. Authorized Use of IT Resources. TMD IT Resources are the property of the U.S. Government and may be used only by authorized TMD personnel for approved purposes. Users are authorized access to their computer system to assist them in the performance of their duties. Occasional limited personal use by authorized users may be permitted if the use does not:

a. Interfere with the user's work performance;

b. Interfere with any other user's work performance;

c. Have undue impact on TMD's IT services, networking systems, information assurance, and communications (voice, video, data);

d. Result in added costs to the government; or

e. Violate any other provision of this policy or DoD guidelines and regulations.

7. Monitoring. The computers, computer accounts, and telephones (analog, digital and cellular) provided to users are to assist them in the performance of their duties. In accordance with (IAW) DoD policy, all communications are subject to monitoring. Passwords and Common Access Cards (CAC) are used to allow access to TMD computers by authorized users; they do not imply or ensure privacy. Users should have NO expectation of privacy, except as described below, in anything they create, store, send, or receive on a Government Information System. The US Government has the right, but not the duty, to monitor any and all aspects of its IT Resources, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users, reviewing e-mail sent and received by users, and monitoring telecommunications.

8. Standard Mandatory Notice and Consent Provision for All DoD Information System User Agreements. (Enclosure I)

a. By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) Information Systems:

(1) You are 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. You 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 (PM), Law Enforcement (LE), and Counter-Intelligence (CI) investigations.

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

(3) Communications using, or data stored on, this Information System 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 System includes security measures (e.g., authentication and access controls) to protect U.S. Government interests and is not for your personal benefit or privacy.

c. 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 products) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work products are private and confidential.

d. 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.

e. The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence 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 negate any applicable privilege or confidentiality that otherwise applies.

f. User’s data maybe subject to release in accordance with The Freedom of Information Act (FOIA) upon legal review.

g. 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 Information System if the user intends to rely on the protections of a privilege or confidentiality.

h. 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.

i. 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.

j. 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.

k. 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.

l. 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 provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

END OF STANDARD MANDATORY NOTICE

9. Prohibited Activities. TMD computer users are prohibited from engaging in illegal, fraudulent, malicious, or inappropriate activities. Examples of these activities include, but are not limited to the following:

a. Engaging in partisan political activity, political or religious lobbying, or advocacy of activities on behalf or organizations having no affiliation with DoD.

b. Using TMD computer resources for personal or commercial financial gain or solicitation of business services. An exception to this prohibition is the sale of personal property on the public electronic bulletin board posted for that purpose.

c. Unauthorized Fundraising. Fundraising activities are governed by The Joint Ethics Regulation and are generally prohibited. All such requests will be submitted to the Office of the General Counsel, TMD, for prior approval.

d. Viewing, downloading, storing, transmitting, or copying materials that contain sexually explicit or sexually oriented images, or text.

e. Creating, copying, accessing, storing, processing, displaying, or distributing fraudulent, harassing, embarrassing, intimidating, defamatory or any other material that is intended to be offensive to any member or employee of the TMD, National Guard Bureau, Department of the Army, Department of the Air Force, or Department of Defense (for example: hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin, or sexual orientation).

f. Obtaining, installing, reproducing, or distributing software and data, in violation of intellectual property rights or license.

g. Personally-owned hardware, e.g., PDAs, may not be attached to any government computer network or to a government owned computer under the control of the TMD without the express written approval of the TMD CIO/DOIM or their authorized delegate, and only then, will the installation be accomplished by authorized TMD J6 personnel.

h. Copying software for use on home computers. If there is a valid requirement to do so, CIO staff will provide copies for authorized users to check out.

i. Making any unauthorized alterations to any TMD automation system hardware by misusing local administrator privileges, to include changing any system option, setting or default.

j. Creating, copying, or electronically transmitting chain letters, or other non-mission-related mass mailings. A chain letter is a message sent to a number of people asking each recipient to send copies with the same request to a specified number of

addressees. A mass mailing is a message sent to a large number of recipients, such as the TXALL address group, without any legitimate business purpose.

k. Electronically transmitted messages that deal with TMD personnel and activities are considered as having a legitimate business purpose.

l. Performing acts that waste computer/network resources or unfairly monopolize these resources to the exclusion of others. These acts include sending or receiving e-greeting cards, music and video files, interactive games or other large file attachments; subscribing to Internet services that automatically download information (sports scores, stock prices, or other continuous data streams such as music or videos); spending excessive amounts of time on the Internet for non-mission-related purposes; instant messaging (other than AKO); on-line chat groups (other than AKO). Any technology that provides business collaboration or instant messaging capabilities will be approved through the J6 change control board management process.

m. Using TMD IT Resources as a staging ground or platform to gain unauthorized access to other systems.

n. Incurring any network or phone charges for which the US Government is liable, except for official purposes.

o. Providing copies of software to a third party.

p. Use of shared drives (to include eLSP) to store, maintain or relay Privacy Act data (such as PII), unless the data is password protected, and the folder within the shared drive has restricted access to those with a need-to-know authorization. Additionally, any release of TMD names or e-mail addresses to second or third parties may only be for official business and should be coordinated with the owner beforehand.

q. Installing software onto any TMD IT Resource without specific approval and authority to do so as approved by TMD CIO/DOIM or an individual delegated the authority to make such approval.

10. Password Security. All accounts that do not use the Common Access Card to authenticate identity when logging into a system must be password protected. Passwords must comply with the length and content standards established at the time the account is created and will require regular updates to avoid automatic expiration. Frequency intervals of password changes are prescribed by DoD policy and cannot be waived. Passwords must never be shared with anyone. Accounts configured for User Based Enforcement (UBE) of Public Key Infrastructure credentials do not use passwords and are exempt from this provision.

11. Public Key Infrastructure (PKI).

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

b. Token/Smart Card (or CAC). The Cryptographic Common Access Card Logon (CCL) is the primary access control mechanism for all Army users

c. Digital Certificates (Private/Public Key). CAC is used as a means for sending digitally signed e-mail and encrypted e-mail. 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), or if a hyperlink is included as part of the text of the message. The digital signature serves both as a measure of confidence to the receiver that the signer is the one and only person who could have sent the e-mail as well as a non-refutable indicator that the sender cannot later recant having originated the e-mail.

d. Public Key is used to encrypt information and verify the origin of the sender of an e-mail. 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), and on any e-mails sent from one General Officer to another General Officer.

12. Removable Storage Media (CDs, DVDs, Diskettes, etc.). All users must assess the risk of using removable storage media, apply appropriate controls and mitigate residual risk of compromising classified and/or sensitive information stored on removable media. While these media have multiple uses and their small size makes them very convenient and adaptable, recent events have proven that without proper safeguards these devices can prove to be a sizable vulnerability to DoD networks and the information stored and moved therein. Removable media will be subject to additional security controls as mandated by Information Condition (INFOCON) security levels. NOTE: USB thumb drives or any other USB storage device is unauthorized.

13. Data-at-Rest. Mobile computing devices will be encrypted utilizing the Microsoft BitLocker or other Army authorized encrypting software or as directed by the TMD DOIM/CIO.

14. Wireless Systems. Wireless systems provide a cost-effective solution for extending wired networks to remote areas. However, wireless systems also provide an easy means of hostile exploitation, such as when unauthorized wireless access points are installed.

a. Installation of wireless access points (stand alone or connected to Army network) without prior approval from the Directorate of Information Management (DOIM) is strictly prohibited.

b. The ISSM will periodically scan for wireless networks on the installation. Unauthorized wireless systems will be shut down on the spot and equipment confiscated.

c. Wireless networks must be secured utilizing encryption. Wireless systems will conform to appropriate Army best business practices and configured for a minimum of FIPS 140-2 encryption.

d. At no time will any access point be installed in offices as an extension to connect additional computers or printers without prior approval from the DOIM

e. Wireless networks must operate in conjunction with an approved wireless network security solution to reduce the likelihood of hostile exploitation of the TMD by rogue devices.

15. Peer-to-Peer (P2P) and Instant Messaging. Use of P2P and (non-AKO) Instant Messenger programs on the TMD network is strictly prohibited. P2P places all network resources at risk due to file sharing use. Viruses, Trojan Malicious Code, and Spyware programs are often spread using these types of file sharing programs. No P2P file sharing is authorized for download, installation, or use on any government system. Examples of this type of file sharing software include Kazaa, Morpheus, Gnutella, Grokster, Lime Wire, BearShare, Skype and other popular music/data sharing programs. Instant Messenger programs can bypass security protocols allowing an avenue of approach for malicious code. Examples of unauthorized Instant Messenger programs include AOL Instant Messenger (AIM) and Yahoo Instant Messenger.

16. User Responsibilities.

a. Protect and defend information and Information Systems (IS) by ensuring their confidentiality, integrity, availability, authentication and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection and reaction capabilities.

b. Protect hard copy produced at the sensitivity level of TMD owned IS until reviewed for proper classification or sensitivity and control.

c. Destroy information or media, when required, IAW security requirements based on the level of classification or sensitivity.

d. Provide access to sensitive information after ensuring the parties have the proper authorization and need-to-know.

e. Operate the IS only in areas approved for the highest classification or sensitivity level of the information involved unless specific authorization has been received from the CIO/Information System Security Manager (ISSM) to operate the computer in other areas.

f. Never remove the computer or its hard drive from TMD facilities without specific approval of the supervisor and coordination with the Information Management Officer (IMO). In the case of laptop computers, a signed hand receipt must be on file with the issuing organization.

g. Comply with terms of software licenses and only use TMD licensed and authorized software.

h. Use TMD systems for lawful, official, use, and authorized purposes IAW current guidelines.

i. Use the e-mail system IAW DoD and TMD guidelines. Limit distribution of e-mail to only those who need to receive it.

j. Properly mark and label sensitive media IAW DoD and TMD policies. Ensure sensitive information is removed from hard disks that are sent out for maintenance.

k. Activate screen-lock on the computer or log off when leaving the work area, and restart/log off computers at the end of each day.

l. Complete an annual Information Assurance (IA) awareness training or refresher and provide proof of the same to the supporting Information Technology Agent (ITA) or as directed by the TMD DOIM/CIO. Accounts expire annually, therefore, a new IA training certificate must be submitted for account renewal.

m. Annually read and acknowledge this Acceptable Use Policy.

n. Sign logs, forms, and receipts as required/applicable for accomplishment of duties relating to the collection, use, transfer or disposal of TMD information or IS.

o. Report known or suspected incidents immediately to the ISSM either via-email, via-phone or via-service desk ticket and immediately report any evidence of tampering with the computer or its seals.

p. Notify the ISSM when access to the computer is no longer needed, e.g., upon transfer, termination, leave of absence, or any period of extended non-use.

q. Provide physical access to mobile devices (e.g. Laptops) upon request for inspection for security purposes.

r. Log off and maintain power to all Information Systems in order to facilitate automated maintenance, patching and upgrading during non-business hours.

17. The Point of Contact for this memorandum are MSG Melanie Zoerman, Information Systems Security Manager at 512-782-1102 or melanie.j.zoerman.mil@mail.mil.

HEISER.BILLIE.WAYNE.II.1132333625
Digitally signed by HEISER.BILLIE.WAYNE.II.1132333625
Date: 2018.10.05 09:59:30 -05'00'

Enclosure

BILL W. HEISER, II
LTC, GS, JFHQ
Director, CIO/J6