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

MEMORANDUM FOR All Office of State Administration

SUBJECT: Information Technology (IT) Acceptable Use Policy (AUP) and User Responsibility Agreement Applicable to State-owned Resources

1. References. Department of Information Resources, Texas Administrative Code 202 (TAC 202).

2. Purpose. To promulgate policy regarding the authorized uses of State IT Resources within or under the control of the Office of State Administration (OSA) to ensure that information and computer systems are used responsibly, professionally, ethically, and legally.

3. Applicability. This policy applies to any person who in the course of their duties under the control of the Adjutant General of Texas, and with the approval of the State Information Resources Manager (IRM), accesses OSA IT Resources. Violations of this policy may result in disciplinary action which can include administrative punishment and/or criminal prosecution.

4. Definitions.

IT Resources covered under this AUP refer to all OSA State-owned or supported network and communications systems and devices. OSA IT Resources include, but are not limited to, host computers, file servers, application servers, mail servers, web servers, communications servers, workstations, stand-alone computers, laptop computers, agency state-issued cell phone devices, tablets, and all internal and external communications networks accessible directly or indirectly from the OSA computer network. OSA IT Resources refer to both classified and unclassified information processing and include both normal operating environments and emergency communications environments.

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

b. The OSA Information Security Officer (ISO) is responsible for the State Information Assurance (IA) program and Cyber Security of the State Information System (IS) within the State network environment (NE). OSA's State ISO performs a variety of security related tasks including the development and implementation of system information security standards and procedures. The agency's State ISO ensures that the State IS are functional and secure within the State NE.

c. Emergency Communications are normally utilized during an identified period of response to manmade and natural disasters.

d. 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. Criminals potentially can exploit PII 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.

5. Authorized Use of State IT Resources. OSA`s IT Resources are the property State of Texas and may be used only by authorized OSA personnel for approved purposes. Users are authorized access to their State 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 OSA's IT services, networking systems, information assurance, and communications (voice, video, data);

d. Result in added costs to the agency; or

e. Violate any other provision of this policy or TAC202 guidelines and regulations.

6. Monitoring. State-issued computers, computer accounts, and cell phones provided to users are to assist them in the performance of their duties. Login credentials are used to allow access to OSA 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 State Government Information System. The agency has the right, but not the duty, to monitor all aspects of its State-issued IT Resources, including, but not limited to, monitoring internet sites

employees visit, chat groups and news groups, material users download or upload, email (sent and received), and telecommunications.

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

a. By signing the user agreement, the user acknowledges and consents that when accessing OSA`s Information Systems, he or she is accessing a State Government Information System (which includes any device attached to this Information System) that is provided for State Government authorized use only.

b. The user consents to the following conditions:

(1) Department of Information Resources (DIR) and OSA ISO routinely intercepts and monitors data communications on this State Information System for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network operations and defense.

(2) At any time, the OSA may inspect and seize data stored on this State Information System if fraudulent activity is detected.

(3) Communications using, or data stored on this State Information System are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any agency authorized purpose.

(4) This State Information System includes security measures (e.g., authentication and access controls) to protect OSA`s interests and is not for individual personal benefit.

c. Notwithstanding the above, using a State Information System does not constitute monitoring of the content of privileged communications or data (including work products) that are related to personal representation or services by attorneys. 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 OSA`s actions for purposes of network administration, operation, protection, defense, or for communications security. This includes all communications and data on a State 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, fraud, and cyber-attack investigation). However, consent to interception/capture or seizure of communications is not consent for the investigator to use privileged communications for fraudulent purpose.

f. User data and information may be subject to release upon legal review in accordance with the State's Public Information Act or the federal Freedom of Information Act.

g. Whether any 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 OSA policy. Users are strongly encouraged to seek personal legal counsel on such matters before using a State 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 OSA 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 OSA policy. However, in such cases OSA 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, OSA 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, cyber-attack, or fraud 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), OSA may, solely at its discretion and in accordance with its policy, elect to apply a privilege or other restriction on OSA's otherwise-authorized use or disclosure of such information.

l. All the above conditions apply regardless of whether the access or use of a State 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.

8. Prohibited Activities. Users of State-issued computers 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 of organizations having no affiliation with OSA.

b. Using OSA computer resources for personal or commercial financial gain or solicitation of business services.

c. Unauthorized fundraising—fundraising activities are governed by ethics regulations and are generally prohibited.

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 OSA (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. Attaching personally owned hardware, e.g., tablets, cellphones, etc., to any State government computer network or to a State government-owned computer under the control of the OSA without the express written approval of the ISO or IRM; authorized OSA IT personnel will only complete installation if the ISO or IRM issues written approval.

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

i. Making any unauthorized alterations to any OSA 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. A chain letter is a message sent to several 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 many recipients, such as the TXALL address group, without any legitimate business purpose.

k. Performing acts that waste computer/network resources or unfairly monopolize these resources to the exclusion of others. These acts include sending or receiving large files; downloading or streaming 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-agency-related purposes; spending time on Facebook and other social media platforms. Any State-related technology that provides business collaboration or instant messaging capabilities will be approved through the ISO`s office change control board management process.

l. Using OSA's IT Resources as a staging ground or platform to gain unauthorized access to other systems.

m. Incurring any network or phone charges for which OSA is liable, except for official purposes.

n. Providing copies of software to a third party.

o. Using shared drives (to include SharePoint) 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 OSA names or e-mail addresses to second or third parties may only be for official business and should be coordinated with the owner.

p. Installing software onto any OSA IT Resource without specific approval and authority to do so as approved by OSA ISO or IRM.

9. Password Security. All accounts will be authenticated using password, username, and multifactor authentication to identify the user. 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 OSA access control policy and cannot be waived. Users must never share passwords with anyone.

10. Removable Storage Media (CDs, DVDs, flash drive, 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. These media have multiple uses, and their small size makes them very convenient and adaptable; however, recent events have proven that without proper safeguards, these devices can prove to be a sizable vulnerability to OSA`s network and the information stored and moved therein. Removable media will be subject to additional security controls as mandated by the ISO. USB thumb drives and other USB storage devices are NOT authorized for use.

11. Data-at-Rest. Mobile computing devices will be encrypted utilizing the Microsoft BitLocker authorized encrypting software or as directed by the OSA's ISO and IRM.

12. 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 OSA network) without prior approval from the IRM is strictly prohibited.

b. The ISO will periodically scan for wireless networks. Unauthorized wireless systems will be shut down and equipment confiscated.

c. Wireless networks must be secured utilizing encryption. Wireless systems will conform to appropriate 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 to a State network without prior approval from the IRM.

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

13. Peer-to-Peer (P2P) and Instant Messaging. Use of P2P and (non-OSA) Instant Messenger programs on OSA 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 State 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.

14. User Responsibilities. Users are obligated to:

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

b. Protect hard copy information at the appropriate sensitivity level until reviewed for proper classification or sensitivity and control.

c. Destroy information or media when required with appropriate approval from the ISO or such designated authority.

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

e. Operate the SIS only in areas approved for the highest classification or sensitivity level of the information involved unless specific authorization has been received from the ISO and IRM to operate the computer in other areas.

f. Never remove State computer or its hard drive from OSA facilities without specific approval of the supervisor and coordination with the IRM. In the case of laptop computers, a signed hand receipt must be on file with the issuing organization.

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

h. Use OSA systems for lawful, official use, and authorized purposes according to OSA guidelines.

i. Use the e-mail system provided by OSA and within OSA guidelines. Limit distribution of e-mail to only those who need to receive it.

j. Properly mark and label sensitive media according OSA 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 and provide proof of completion to the ISO. Annual training will be completed once every fiscal year.

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 OSA information or SIS.

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

p. Notify the IRM 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 State Information Systems to facilitate automated maintenance, patching and upgrading during non-business hours.

15. The Point of Contact for this memorandum is Frank Oduro, Information Resources Manager at 512-782-3317 or frank.oduro@military.texas.gov

Enclosure

Shelia. B. Taylor
Office of State Administration Director