CLEET Information Technology Policy

CLEET - Information Technology Division

December 2009

1 Scope and Overview

The CLEET Information Technology Policy details the minimum expectations and requirements accepted by organization for the use of its computing resources by individual users. These guidelines are part of the Information Technology Policy, Standards and General Practices and are updated at a minimum on a yearly basis as required by the State of Oklahoma's Informational Technology Guidelines

This policy is applicable to all users (including contracted personnel) regardless of the system used. In general, these directives apply to all users of:

Hardware: Computing, network and telecommunications equipment, and data centers.
Software: Computing applications supported by the CLEET IT department.
Information: Electronic data and information.

In general, IT provides users with the computing resources necessary to provide added value to the organization. They include personal computers and software, networked computing, electronic mail services and internet access among others. Such resources are the property of , as well as the all information stored, sent or received on such systems, including e-mail and all electronic communications.

Use of any computer resources and systems is accompanied by a significant responsibility to follow this policy. Personal use is acceptable but should be reasonable, professional, ethical, incidental and respectful of other policies such as the Code of Conduct and local laws and regulations.

CLEET is not liable for incidental, consequential, punitive or other damages or a loss of anticipated benefits or profits, resulting from, related to, or arising out of the use of its computing equipment, unless otherwise stated by the local law.

2. Audience

This document is intended as a guide for the following key stakeholders:

System Users: Also referred as "end-users" are regular users of computing equipment and applications. Users employ these practices to understand their responsibilities towards computing equipment, systems and electronic data storage and communications.

CLEET IT Leaders: Use this document to provide IT Security Awareness in their organizations

CLEET IT System Administrators, Operators, Engineers and Program Developers: Use it to understand accepted control practices in regard to accepted use of computing systems.

Auditors: Use it to evaluate compliance of the different organizations with accepted control practices in regard to accepted use of computing systems.

3. Reporting Security Problems

Appropriate CLEET Management must be notified immediately (usually notifying both the user's direct manager and the local CLEET IT manager will be adequate) in the event of loss or disclosure of sensitive information to unauthorized parties, and / or unauthorized use of any ' information systems has taken place or is suspected.

3.1 False Security Reports

The Internet is plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters which request that the receiving party send the message to other people.

Users in receipt of information about system vulnerabilities should forward it to the CLEET IT Department, who will then determine what if any action is appropriate. Users must not redistribute system vulnerability information.

3.2 Testing Controls

Users must not "test the doors" (probe) security mechanisms at either or other Internet sites. If employees/Cadets probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity. Likewise, the possession of tools for cracking information security is prohibited

4, Individual User CLEET IT Policy

CLEET computer users expressly waive any right of privacy in information they create, store, send or receive on ' computer systems. CLEET may choose to monitor individual computer systems, data and/or electronic mail accounts at any given time without prior user notification.

Use of system resources for soliciting business, selling products, or otherwise engaging in commercial activities is prohibited. Abuse or improper use of the computer systems, data and/or electronic mail accounts in connection with either business or personal use, can be grounds for disciplinary action, including termination of employment/ expulsion from the academy and/or legal action.

Users are responsible for their individual computing equipment (e.g. notebooks and laptops). CLEET expects its users to locate all desktop and portable computers, workstations and phones in safe places, protected from fire, environmental conditions and theft.

When traveling, it is also expected that users do not leave computing equipment unattended and pack it appropriately using heavily padded bags or cases. Portable computers should be never checked as baggage or be left in vehicles for an extended period of time.

Users are also responsible for protecting electronic information in their possession. Any person, who possesses sensitive information, shall be responsible for safeguarding that information.

Each user shall monitor conditions affecting assets, note problems, risks, or exception to ' policies and report them in writing to the appropriate level of management as well as take action to prevent the damage or loss of the asset.

4.1 Data Classification:

CLEET documentation regardless of format (electronic or physical) should be classified and labeled according to the sensitivity of the information and data. The following suggested classification should be followed at a minimum*:*

4.2 Private and Confidential:

This classification applies to the most sensitive business information which is intended strictly for use internal use. Its unauthorized disclosure could seriously and adversely impact its business partners, and/or its customers. Information that would consider being private is included in this classification.

Examples include, but are not limited to:

- CLEET reports and strategy documentation
- Litigation planning - includes communications with in-house and external Counsels.
- Financial reports or accounting statements
- Audit reports
- HR information e.g. payroll and employee performance evaluations.
- User passwords
- Communications with third parties protected under a non-disclosure or confidentiality agreement.

4.3 Internal Use Only:

This classification applies to all other information which does not fit into the above classification. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact , its employees, its business partners, and/or its customers

Examples include, but are not limited to:

- Company telephone directory
- Training materials
- Policy manuals and procedures

4.4 Public

This classification applies to information which has been explicitly approved by management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm

Examples include, but are not limited to:

- Advertisements.
- Job opening announcements.
- Press releases.
- Annual financial report.

4.5 Data Storage

Data processed on users' computing equipment must be protected accordingly to the sensitivity of the information. Users should be aware that there are inherent exposures to information networked drives which include various IT administrative and operator ID's which can access all files stored in networked devices. Users must consider the security exposures of the various storage media and their associated controls before storing information in an electronic format. As a general guidance:

- Store data in file servers either in the individual' file server folder or in shared folders as these are protected within centralized data locations or Data Center facilities and backed up regularly.
- When traveling, attempts should be made to store "Private" and "Confidential" information in encrypted removable media (e.g. CD ROMs, floppies, USB keys or disk pens) rather than storing the data in the individual' hard drive. The use of self-encrypting removable media is strongly suggested.
- "Internal Use Only" and "Public" data is not restricted and may be stored without encryption in any media device. CLET IT recommends the storage of all non-sensitive data in file servers or shared folders as they are backed-up daily.

Alternative protection methods to data encryption might be consider by the user if encryption software is not available, feasible or if it does not comply with local data protection legislation and/or export laws for information, hardware and software across national borders.

Such alternative protective methods include one or more of the following:

- Physical access controls to computing resources(e.g., office and file server rack locks).
- Operating system-based access permissions and software passwords (e.g. Windows file permissions, Microsoft office file passwords).
- Add-on software access control packages.

4.6 Internet Access

CLEET management has deemed the Internet as an important productivity tool and accepts its use through the CLEET network. As with any other computer system or service property of the user is responsible of using it only for legitimate business purposes.

Personal use is acceptable but should be reasonable and incidental and conducted in a responsible, professional, ethical, and lawful manner.

Based on the inherent risk of using internet, users must follow these additional guidelines:

- Internet accounts (e.g. hotmail) are not to be used for the storage of data or the transfer of any internal data within or outside the network.

- Users are prohibited from connecting their individual computing equipment to an external network or Internet (via DSL, cable or modem, even if configured to allow dial-out only) while networking in a CLEET location, unless individually reviewed, documented and duly approved by appropriate CLEET IT management.

- Users must not down-load non-business related software from the Internet as they may contain viruses, worms, Trojan horses, and other malicious software which may damage ' information and systems.

- Internet usage should be moderate (use common sense) as it demands computing network capacity and may limit resources to other users or overload systems.

When connecting to the Network from an unsecured Internet connection (e.g. connecting to through the user' personal internet home connection), users are required to use a Virtual Private Network (VPN) client. Users should never connect or attempt to connect to any unauthorized network (e.g. connecting to a neighbor wireless network).

Users are prohibited from connecting to external networks (including Internet) using dial-up modems connected to workstations while simultaneously connected to a local area network (LAN) or another internal communication network without prior authorization from the CLEET IT Department.

4.7 ***Repair/Upgrade of Hardware and Software***

Users are required to contact the CLEET IT Department Help Desk for all hardware and software support, including equipment installations, repairs, upgrades, moves among others.

Users are not allowed to:

- Install any hardware or software without appropriate consultation to the CLEET IT department and adequate software licensing agreement.
- Download non-business related software from the Internet as they may contain viruses, worms, Trojan horses, and other malicious software which may damage CLEET information and systems
- Use any externally-provided software from a person or organization other than a known and trusted supplier.

Approved anti-virus software will be installed, configured and regularly updated on all individual user computers by the CLEET IT department. Users must notify the CLEET IT department of unprotected workstations, outdated virus-software and any virus findings in their individual computing equipment.

Any unlicensed or unauthorized software found on user computing equipment will be either removed or the proper licensing agreement will be acquired in a timely manner.

4.8 Disclaimer of Responsibility for Damages to Data and Systems

CLEET uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.

In keeping with these objectives, the CLEET IT Department maintains the authority to:

- Restrict or revoke any user's privileges
- Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives..
- Take any other steps deemed necessary to manage and protect its information systems.

This authority may be exercised with or without notice to the involved users. CLEET disclames any responsibility for loss or damage to data or software that results from its efforts to meet those security objectives.

5. Electronic Mail Communications Policy

The CLEET IT department provides users with a common electronic communication system (e.g. Outlook) to meet communication requirements of the organization. Additional electronic communication devices such as Instant Messaging may be prohibited if deemed necessary by the affiliate management. Internet mail accounts (e.g. hotmail) are not to be used for the storage of data or the transfer of any internal data within or outside the network.

CLEET users should treat e-mail and any other electronic messages (including Instant Messaging) as they would treat any formal business document. Electronic communications should be written in accordance with standard business guidelines and conducted in compliance with all policies. Style, spelling, grammar, and punctuation should be appropriate and accurate.

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent or received by e-mail or other form of electronic communication (e.g., Instant Messaging, bulletin board systems, newsgroups and chat groups) or displayed on or stored in any CLEET 's computer systems. Jokes that contain objectionable material may be easily misconstrued when communicated electronically and should be avoided.

While CLEET is not responsible for the receipt of any questionable or inappropriate e-mail or any form of electronic communication, users encountering or receiving this kind of material should report the incident to the appropriate level of management and to the CLEET IT Department. Users should not forward the message to others and should not open or respond to any unsolicited electronic communication.

Users should conserve CLEET's computer resources and colleagues' time. Send electronic messages and copies only to those with a legitimate need to read the message. Chain messages should be deleted, not forwarded, as they can overload the system and limit CLEET IT resources.

System settings prohibit sending organization-wide electronic messages to all employees without approval from appropriate management. In addition, people should not reply to or request replies to organization-wide electronic communications.

5.1 Confidentiality and Electronic Mail Security

Users should exercise sound judgment and common sense when distributing e-mail messages. The confidentiality of third-party messages must be guarded and protected, like any other CLEET confidential material.

Confidential or personal information should never be sent via e-mail without the understanding that it can be intercepted. Copies of your electronic messages, including e-mail, instant messaging, and fax may be forwarded to others either electronically or on paper.

E-mail sent to non-existent or incorrect usernames may be delivered to persons that you never intended. Caution should be exercised when sending confidential or sensitive information; CLEET users are responsible for using the correct media for communication of such material.

Users should never consider electronic communications, including e-mail, instant messaging, or fax, to be either private or secure unless otherwise explicitly stated or encrypted. E-mail may be stored indefinitely on other computers, including that of the recipient.

5.2 Electronic Mail Retention and Mail File Size

System resources must be conserved to maintain system reliability and performance. To reduce systems overload, a mail file (mail box) quota will be applied to all electronic mail users. The size quota will allow the user to decide which electronic mail you want to keep within that limit. Mail accounts that exceed the quota will continue to receive incoming messages, but will not be able to reply to any messages.

Users are required to retain and save any information that is required by legal or regulatory requirements. Requests for addition mail file space will need approval from appropriate CLEET IT management.

As a suggested practice, electronic mail messages should not be retained past 60 days. If a user has messages that are business critical or contain financial information, or are otherwise required to be retain and/or saved due to legal or regulatory requirements, those messages should be filed and saved appropriately by the user.

Retention of messages in Public Folders must be set to the requested period of time as defined by the folder owner. By default all messages will be automatically deleted from such folders after 60 days unless otherwise requested by the owner. The maximum retention period of a public folder is 2 years.

5.3 Non-Employee Electronic Mail Guidelines

When circumstances require non- employees such as consultants, contractors, etc., to have electronic mail access within the system, the non- employee will be required to adhere to the CLEET's Information Technology Policy, in addition to the following non-employee guidelines:

Non- employees must be issued with an electronic mail address that identifies them as non- employees. The contractor user email account format is:

OutsideCompanyName.IndividualFirstName.IndividualLastName@cleet.state.ok.us

Non- employees email accounts must automatically expire after the requested period of time by the business owner. If contract expiration is greater than one year, or is unavailable or unknown, set the account expiration to one year at a maximum.

Non- employees are prohibited from inclusion in any distribution groups and public folders that may contain business sensitive information. E.g. non- employees should not be included in groups for employees only communications – such groups usually include "People" in the name.

Non- employee access to electronic mail is restricted to related correspondence and may be available only during standard business hours.

Non- employees' accounts must be established and maintained in the individual businesses' Guest groups within Active Directory

5.4 Electronic Mail Disclaimer

The following disclaimer will be added to outgoing e-Mail signature block by each user.:

"This communication is for use by the intended recipient and contains information that may be privileged, confidential or copyrighted under law. If you are not the intended recipient, you are hereby formally notified that any use, copying or distribution of this e-Mail, in whole or in part, is strictly prohibited. Please notify the sender by return e-Mail and delete this e-Mail from your system. Unless explicitly and conspicuously stated in the subject matter of the above e-Mail, this e-Mail does not constitute a contract offer, a contract amendment, or an acceptance of a contract offer. This e-Mail does not constitute consent to the use of sender's contact information for direct marketing purposes or for transfers of data to third parties."

5.5 Blackberries and other Handheld Communication Devices Guidelines

CLEET management may deem the use of Blackberries or other handheld devices as an important productivity tool for selected individuals. The CLEET IT Department will provide the supported handheld equipment and associated connectivity to such individuals.

As with any other computer system or service property of , the handheld user is responsible of using it only for legitimate business purposes. Personal use is acceptable but should be reasonable, professional, ethical, incidental and respectful of other policies such as the Code of Conduct and local laws and regulations.

Management is responsible for ensuring that the handheld service consumption by each individual user is adequate. Misuse of assigned handheld devices can result in disciplinary action, including termination of employment/expulsion from the academy and/or legal action.

Based on the inherent risk of using electronic handheld devices, CLEET users must follow these additional guidelines and safety considerations:

- Read and abide by the manufacturers' user manual and safety operation instructions prior operating the handheld device.
- Obey all local laws, regulations posted signs and instructions.
- Do not use data functions such as email, web browsing or text messaging while driving. Always use a hands free device when making calls while driving.
- Only use manufacture approved accessories and parts.
- Turn handheld device off when in any area with a potentially explosive atmosphere or while in an aircraft unless authorized by airline personnel.

Most electronic equipment is shielded from the low-level Radio Frequency (RF) energy that is emitted by the handheld devices. However, RF energy may affect some malfunctioning of improperly shielded electronic equipment. Users should consult a physician or the device manufacturer on the effect of RF signals on any medical condition one may have, e.g. pacemakers, hearing aids, etc.

6. Strong Password Policy

Electronic passwords are an important part of computer system security. It is the user responsibility to maintain the secrecy of his/her password. Misuse of passwords, the sharing of passwords, and/or the unauthorized use of another employee's password can result in disciplinary action, including termination of employment/expulsion from the academy and/or legal action.

A user may be held accountable for any activities and actions performed using their accounts even if password was shared.

The following are guidelines concerning electronic passwords:

- Password must contain at least six characters
- Contain characters from two of the following three groups:
    - Letters (uppercase and lowercase) A, B, C... (and a, b, c...).
    - Numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
- Be significantly different from prior passwords.
- Not contain your name or user name.
- Not be a common word or name.

- Passwords will automatically lock after a maximum of seven failed consecutive access attempts
- Application owners could request lower intervals if system risk is high.

CLEET IT suggests the following common sense guidelines to help protect user passwords:

- Do not leave a copy of your password where someone else might find it.
- Change passwords at a minimum every three months.
- Do not use family or pet's names, your initials, phone number, address or birthday as a password as they are easily guessed.
- Passwords that have been compromised or suspected of being compromised should be changed immediately and the event notified to the CLEET IT Department
- CLEET IT Manager or his/her designee will be responsible in manually forcing password changes be made on Jan 1st, Apr 1st, Jul 1st and October 1st for all Logon ID monitored by CLEET IT staff. This will be accomplished thru the Active Directory on CLEET servers.

7. Virus and Malicious Software Prevention

Viruses and malicious software are programs or code segments that are self-replicating and require a host or executable disk segments. In general viruses transmit from machine to machine by any mean of electronic communication or data sharing and are intended to destroy data or render a PC or network unusable. In some cases, this kind of malicious code is use to steal data inadvertently from the infected user or network. The following guidelines must be followed for all ' computing systems:

- Approved anti-virus software must be installed, configured and regularly updated on all individual user computers
- Users must notify the appropriate CLEET IT department of unprotected workstations, outdated virus-software and any virus findings. Corrective actions must be taken in a timely manner
- Users must not download non-business related software from the Internet as they may contain viruses, worms, Trojan horses, and other malicious software which may damage ' information and systems.
- Users must not use any externally-provided software from a person or organization other than a known and trusted supplier

---

Reviewed and approved by Kimberly Richey Assoc. Dir of Admin/General Council - 01/02/2010

Authorized by Dr. Larry Birney, CLEET Executive Director 01/04/2010

C.L.E.E.T Acknowledgement Form

I _____ have received a copy of the CLEET IT Users Policy and agree to abide by the Policy as it pertains to all of my computer usage, by whatever means I connect to the CLEET data network. These means may include, but are not limited to the CLEET Computer Resource Center, any administrative or Staff computer systems, or my personally owned computer while connecting through the CLEET network.

I understand that the contents of the CLEET IT User Policy may expand and/or change, and that CLEET IT Staff will communicate these changes to personnel via e-mail and CLEET Website.

I agree to continue to abide by the terms and conditions for CLEET IT Users Policy in its original and/or changed form.

Signature X_____ Date ___/___/_____