	Effective Date: November 02, 2010 Revision Date: **Bastrop County Emergency Services District No.1** **Standard Operating Procedures**

Title: **Computer Use**

Originator – Fire Chief (Signature/Date): _____ _____

PURPOSE

To ensure responsible and acceptable use of computers by all members of the Bastrop County Emergency Services District No.1 according to the Bastrop County Emergency Services District No.1 Employee Handbook ***Section 4002 Internet Policy***.

GENERAL

Internet facilities are to be used for business purposes only. Member use of the Internet is viewed as a privilege and not a right.

POLICY

Members are subject to disciplinary action up to and including indefinite suspension for unacceptable use of computer resources, including email and Internet usage. Some examples of unacceptable uses that could result in termination include: conducting or promoting a commercial or personal business; engaging in political lobbying; viewing or receiving sexually explicit material; sending racial, ethnic, religious or gender-based slurs; and threatening or harassing others. In addition, all members should be aware that Internet usage and email messages are not personal or private. All computer files are the property of the Bastrop County Emergency Services No.1 and, therefore, a public record. It is the department's responsibility to ensure departmental computer usage is monitored and access is limited to each individual; however Bastrop County Emergency Services District No.1 will perform periodic audits of content and computer performance.

PROCEDURE

A. Computer Acceptable Use

1. The use of ESD-provided Internet, e-mail and/or computer use must be related to, and for the benefit of the ESD or Department. Similar to the use of telephones, televisions, and newspapers, computers are a major instrument for communications within our society. Limited personal use may be permitted, as approved by the ESD Fire Chief, at times when the use does not interrupt, interfere or prevent the productivity of ESD business or work requirements. All personal use of the computer must be appropriate for the workplace. Any questions should be directed to the immediate supervisor.

2. All on-line communications, such as electronic mail messages (and attachments) and postings to various kinds of discussion groups, are subject to the same laws, regulations,

policies, and other requirements as information communicated in other written forms and formats. This includes proper business correspondence practices and proper use of Bastrop County Emergency Services District No.1 equipment and resources.

3. Use network resources responsibly to avoid having a negative impact on others who need to share those resources.

4. User Responsibilities

a. Comply with this "Acceptable Use Policy." By participating in the use of networks and systems provided by the ESD, users agree to comply with ESD and department policies governing their usage.

b. Do not download and/or install non-authorized software on PC.

c. Take all reasonable precautions to prevent the use of their electronic mail account and their workstation by unauthorized individuals. Lock or use a screen saver password whenever you leave the PC to protect your account from unauthorized access.

d. Users are responsible for activity from their login account, email account and/or their workstation.

e. Comply with other ESD and department policies, procedures, and standards.

f. Be courteous and follow accepted standards of etiquette and "netiquette".

g. Use information technology resources efficiently and productively.

h. Communicate data security needs of information under your purview to your Chief or the ESD Chief.

i. All desktops must have up to date virus protection installed and active.

j. All servers should have up to date virus protection. If you feel like you have a server that does not require it, please email info@bastropesd1.com

k. Save all business data to authorized drives that ensure backups are done appropriately.

l. Do not share passwords. Do not give your password to anyone. Authorized users will be able to get your password through legitimate means. (For example: If your IT person needs to access your account, they have the rights to change your password.) You are responsible for your login account and password.

5. Privacy

a. Neither Internet usage nor electronic mail messages are personal or private.

b. All computer files are the property of the ESD, regardless of their physical location or the form in which they are maintained. The ESD reserves the right to access and disclose all messages and other electronic data, sent over its electronic mail system or stored in its files, for legal and audit purposes. Under the Texas Open Records Act, any electronic mail can be a public record. Employees should be aware that electronic records are subject to the mandatory public disclosure requirements of the Texas Open Records Act, subject to the exceptions under the Act.

c. E-Mail is backed up daily on a permanent basis allowing the ESD to restore current electronic mail in the event of system failure. Employees should assume that copies (back-up copies or otherwise) of electronic mail messages and other electronic correspondence may exist on other systems even though the sender and recipient have discarded their copies of the document.

d. The department is responsible to ensure that every connection to the Internet is monitored or subject to audit (all email, web sites, instant messages, etc.)

6. Acceptable uses of computer resources are those that conform to the purpose, goals, and mission of the department/ESD and to each user's job duties and responsibilities. The following list, although not all-inclusive, provides some examples of acceptable uses:

a. Communications and information exchanges directly relating to the mission, charter, and work tasks of the department including electronic mail in direct support of work-related functions or collaborative projects.

b. Communications with vendors of products used or being considered for use by the ESD, either to investigate use of their product or to receive help in using their product.

c. Communications, including information exchange, for professional development or to maintain job knowledge or skills.

d. Announcements of ESD laws, procedures, hearings, policies, services, or activities.

e. Use involving research and information gathering in support of the ESD’s governmental duties.

7. Unacceptable use can be defined generally as activities that do not conform to the purpose, goals, and mission of the ESD/department and to each user's job duties and responsibilities. Any computer usage in which acceptable use is questionable should be avoided. When in doubt, seek policy clarification prior to pursuing the activity.

8. The ESD computer use, e-mail and/or Internet access may not be used to:

a. Listen to, view, or temporarily download audio or video files for entertainment or leisure activities during normal business hours. These activities are bandwidth intensive and take resources away from our users.

b. Seek or gain unauthorized access to ESD network resources or to Internet resources.

c. Destroy the integrity of computer based information.

d. Compromise the privacy and/or security of users.

e. Disrupt the functions of ESD networks or other computer resources, including, but not limited to, propagation of worms or viruses or other debilitating programs.

f. Conduct or participate in illegal actions.

g. Violate ESD or fire department policies.

h. Circumvent legal protection provided by copyright and license to programs and data.

i. Conduct or promote commercial or private/personal business enterprises or products.

j. Engage in political lobbying.

k. Support or solicit on behalf of groups, organizations, etc. that are not related to the ESD.

l. Transmit unsolicited commercial information (i.e. junk mail, advertising, etc.)

m. Transmit material that may be deemed offensive to its recipient.

n. View, transmit, or receive sexually explicit material.

o. Advocate racial, ethnic, religious, or gender-based slurs.

p. Threaten or harass others.

q. Harm to minors.

r. Threats.

s. Harassment.

t. Fraudulent activity.

u. Forgery or impersonation.

v. Unsolicited email or bulk email.

w. Unauthorized access.

x. Copyright or trademark infringement.

9. Anyone who inadvertently encounters an unauthorized site or inappropriate email receipt is to immediately sever the site linkage and/or delete the file. Upon such an occurrence, the member is to notify their immediate supervisor acknowledging the inadvertent site contact and the approximate time and duration the site was visited. An email should be sent through the member's chain of command to the Chief level to document the incident

10. The ESD realizes that we have little control over communications received, especially those received from unsolicited sources. Any unsolicited electronic correspondence (spam) should be deleted.

B. Use of Personal Software and Hardware

The use of ESD/Departmental provided hardware and/or software is prohibited without approval from the ESD Chief.

C. Prohibited Applications and Devices

No privately owned computing device (laptop, tablet PC, mobile device, etc.) shall be connected in any way to a ESD computer or network unless previous permissions have been granted by ESD Chief. Bastrop County Emergency Services District No.1 is not responsible for damage or theft of privately owned computing devices. Private devices used while on ESD property are subject to all provisions of the Computer Acceptable Use policy.

D. Prohibited Email Attachments

Email is one of the primary vectors for the transfer of malicious software. Refer to the ESD's Acceptable Use Policy to ensure that the files being transferred are in conformance with the acceptable uses of computer equipment in the ESD.

E. BCESD No.1 Removable Media

1. Steps must be taken to minimize the risk of data lost or stolen on all removable media (i.e.: floppy disks, removable hard drives, usb flash drives, cdroms, dvds, etc.) which contain confidential information for the ESD, especially Electronic Personal Health Information (EPHI) and/or Electronic Protected Information (EPI).

    a. Members with access to this type of information shall physically secure all removable media when not in use. This can be accomplished by placing the media in a locked container such as a safe, locked office, locked desk, locked filing cabinet, as long as the container cannot be easily removed.

    b. All EPI and/or EPHI information must be encrypted if it is stored on removable media and is not physically secured.

F. BCESD No.1 Handheld Device Use

Handheld Devices must not be used to store EPI and/or EPHI data. All Handheld Devices must utilize the ESD's standards for encryption for the data being transferred and must utilize the ESD's standards for password protection. The member must exercise the ESD's physical controls on the portable device.

G. Information Security Sanctions

Workforce members who violate the information security policies of the ESD will be subject to loss of ESD resources and/or disciplined in accordance with the severity of the infraction and pursuant to the ESD's personnel policies.

H. Instant Messaging

Commercial IM protocols (AIM, Yahoo Messenger, etc) are strictly forbidden for use within the ESD's network infrastructure. Use of IM by ESD members must conform to the ESD's Acceptable Use Policy.

I. Intellectual Property/Social Media

Any written, auditory, and/or visual messages communicated by a member that are relative to the ESD/Department in any capacity are the sole property of the ESD. This includes, but is not limited to, any written, auditory, and/or visual messages communicated via or on ESD resources or via or on personal devices (cell phones, PDAs, etc.) and/or social media (Twitter, Facebook, MySpace, etc.)

J. Screen Locking and Member Log Off

1. All computer workstations attached to the ESD's network must have screen locking software installed which automatically locks or logs off the workstation if left idle more than 15 minutes.
2. Members are ultimately responsible for the security of the computer while logged on. Members must therefore not rely on the 15 minute timeout to lock their system if they are leaving the system unattended, but rather manually lock or log off the computer.