Introduced: _____
Adopted: 5/19/14
Reviewed: _____

Information Technology Policy

OBJECTIVES: To provide appropriate guidelines for accessing and utilizing the internet through the Fire District's network. To provide appropriate guidelines for utilizing email technology that protects the employee and the Fire District.

POLICY: Voice mail, email and internet usage are solely for the purpose of conducting Fire District/Fire Company business.

Any device or computer including, but not limited to, desk phones, tablets, laptops, desktop computers and iPads that the Fire District provides for your use, should only be used for official business. Keep in mind that the Fire District owns the devices and the information in these devices.

INTERNET USAGE Internet use, on Fire District time, is authorized to conduct Fire District business only. Internet use brings the possibility of breaches to the security of confidential Fire District information. Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorized people, outside the Fire District, potential access to Fire District passwords and other confidential information.

Removing such programs from the Fire District network requires IT personnel to invest time and money that is better devoted to other issues.

The following uses of Fire District provided internet access are not permitted:

- To access, upload, download or distribute pornographic or sexually explicit material
- Violate any state, local or federal law
- Vandalize or damage property of any other individual or organization
- To invade or abuse the privacy of others
- Violate copyright or use intellectual material without permission
- To use the network for financial or commercial gain
- To degrade or disrupt network performance
- Access to any otherwise immoral, unethical or non-business-related internet sites

EMAIL USAGE Email is also to be used for Fire District business only. Fire District confidential information must not be shared outside of the Fire District, without authorization, at any time. There will be no personal business conducted on the Fire District email or computer.

Viewing pornography, or sending pornographic jokes, stories or material via email is considered sexual harassment and will be addressed according to our sexual harassment and discipline policies. Any email content that discriminates against any protected classification including age, race, color, religion, sex, national origin, disability or genetic information is prohibited. It is the Fire District policy to also recognize sexual preference and weight as qualifying for discrimination protection. Any employee who sends email that violates this policy will be dealt with according to the harassment and discipline policies.

Keep in mind that the Fire District owns any communication sent via email or that is stored on Fire District equipment. The Board of Fire Commissioners and other authorized personnel have the right to access any material in your email or on your Fire District electronic device at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on Fire District systems.

Any email sent from a Fire District email address will contain the following information: This email was sent from email servers at the Boght Community Fire District. Its contents, including any attachments, are intended only for the individual(s) named. If you received the email in error or from someone who was not authorized to send it to you, do not disseminate, copy or otherwise use it or its attachments. Please notify the sender immediately by reply email and delete this email from your system.

Additional information regarding email usage includes:

- Be suspicious of messages sent by people not known to you
- DO NOT OPEN ATTACHMENTS unless they were anticipated by you. If you are not sure, always verify the sender is someone you know and that he/she actually sent you the email attachment
- Do not forward chain letters. Simply delete them
- Electronic messages can never de unconditionally or unequivocally deleted. The remote possibility of discovery always exists
- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want read aloud in a court of law
- Employees are prohibited from unauthorized transmission of Fire District confidential information or privileged communications

PASSWORD SECURITY Maintaining security of the Fire District's business applications, software tools, email, network facilities and voice mail are critical in providing data integrity and stability of our systems. Passwords are used to limit access to these Fire District assets on an as needed basis.

It is the responsibility of each individual user to protect and keep private any and all passwords issued to them by the Fire District or other authorized personnel.

Password guidelines include:
Select a wide password

To minimize password guessing:

- o Do not use any part of the account identifier (username, login ID, etc.)
- o Use 8 or more characters
- o Use mixed alpha and numeric characters

o Use two or three short words that are unrelated Keep your password safe

- o Do not tell your password to anyone
- o Do not let anyone observe you entering your password
- o Do not display your password in your work area or any other highly visible place
- o Change your password periodically
- o Do not reuse old passwords Additional security practices

o Ensure your computer or log on is reasonably secure in your absence from your work area. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the area

PHONE USAGE The Fire District phone system is an asset to assist in conducting Fire District business. The phone system and equipment are provided to enhance employee capabilities and are not to be construed as assets available for personal use.

During business hours, all calls should be answered within three rings. Be courteous and considerate when representing yourself and the Fire District when using Fire District phone services.

The Fire District phones should be answered as follows: “Boght
Fire Department, (rank) (name), how may I help you?”

BUILDING SECURITY AND ACCESS The Fire District provides keys and access media for use by the employees to maintain building and office security and to allow access to designated areas for authorized personnel.

Physical security of Fire District employees and assets is a primary objective of the Fire District. This policy is intended to help provide a safe and secure work environment, prevent theft and to provide a procedure for appropriate distribution and collection of keys and access media.

The building shall be secured at all times and unlocked only by authorized personnel for approved times. Windows and doors will be locked anytime the building is vacated of personnel. Office doors shall remain locked and closed at all times, unless occupied by authorized personnel.

All keys and access media are the property of the Fire District. The Board of Fire Commissioners, or other authorized personnel may request keys or access media for authorized employees and will be responsible for collecting the keys and access media upon an employee separating from the Fire District. Keys and access media will be assigned by employee name. Each individual assumes responsibility for protecting the security of his/her key and access media and will report losses or situations that possibly jeopardize building security to an officer immediately.

The following actions are a violation of this policy:

- Loaning keys without authorization
- Duplication of keys
- Altering keys, locks or mechanisms
- Admitting unauthorized persons into the building
- Failure to return a key when requested by an authorized person, or upon leaving the Fire District

SOFTWARE USAGE This policy is intended to ensure that all Fire District employees understand that no computer software may be loaded onto or used on any computer owned by the Fire District unless the software is the property of or has been licensed by the Fire District.

Software purchased by the Fire District or residing on Fire District owned computers is to be used only within the terms of the license agreement for that software title. Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the Fire District's Software Usage Policy.

To purchase software, employees must obtain the approval of the Fire District and follow the same procedures used for acquiring other Fire District assets.

Under no circumstances will third party software applications be loaded onto Fire District owned computer systems without the knowledge of and approval of the Board of Fire Commissioners or other authorized personnel.

All software will be used in accordance with its license agreement.

Legitimate software will be provided to all employees who need it. Fire District employees will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to discipline, including up to termination.