L. Bribes, Kick-Backs and any Other Form of Improper Payment

Bribes, kick-backs and any other form of improper payment and services to or from any individual with which the City does business (in any form and for any purpose) are prohibited.

M. Personal Conduct

Care should always be taken to use good judgment and discretion in carrying out the City's business. The highest standards of ethical conduct should always be used.

N. Criminal Matters

Any employee who is charged and/or convicted of a felony, or convicted of a misdemeanor, must immediately notify the City Manager of this fact.

O. Inspection

The City reserves the right to reasonably search any employee or person entering on its property or off-site while performing services for the City, and to search property, equipment and storage areas including, but not limited to, clothing, personal effects, vehicles, buildings, rooms, facilities, offices, parking lots, desks, cabinets, lunch and equipment boxes or bags and equipment. Any items which you do not want to have inspected should not be brought to work.

An employee's consent to a reasonable search is required as a condition of employment and the employee's refusal to consent may result in disciplinary action, including discharge, even for a first refusal.

P. Technical Resource Acceptable Use Policy

1. Introduction

The City's technical resources - including desktop, portable computer systems, tablets, telephones, including cell phones, fax machines, Internet and World Wide Web (Web) access, voicemail, e-mail, intranet and electronic bulletin boards - enable employees quickly and efficiently to access and exchange information throughout the City and around the world.

This policy applies to all technical resources that are owned or leased by the City, that are used on or accessed from City premises, or that are used for City business. This policy also applies to all activities using any City-paid accounts, subscriptions, or other technical services, such as Internet and Web access, voicemail, and e-mail, whether or not the activities are conducted from City premises.

2. Warning

As you use the City's technical resources, it is important to remember the nature of the information created and stored there. Because they seem informal, e-mail messages, voicemail messages and messages posted on the Internet are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. However, even after you delete these messages or close a computer session, the information may still be recoverable and may even remain on the system. You should keep this in mind when creating e-mail messages, voicemail messages, messages on the Internet, and other documents on the computer.

3. Acceptable Uses

The City's technical resources are provided for the benefit of the City and its citizens, vendors, and suppliers. These resources are provided for use in the pursuit of City business and are to be reviewed, monitored, and used only in that pursuit, except as otherwise provided in this policy.

Employees are otherwise permitted to use the City's technical resources for occasional, non-work purposes. Any personal use must be kept to a minimum and may only be conducted during non-work time. Nevertheless, employees have no right of privacy as to any information or file maintained in or on the City's property or transmitted or stored through the City's computer, voicemail, e-mail, or telephone systems.

4. Unacceptable Uses

The City's technical resources must not be used for personal gain. Employees who wish to express non-work related personal opinions on the Internet are encouraged to obtain a personal account with a commercial Internet service provider and to access the Internet without using City resources. Employee postings unrelated to work are not permitted on any type of City electronic bulletin boards or intranet.

Solicitation for any non-City business or activities using City resources during work time is strictly prohibited. Your use of the City's technical resources must not interfere with your productivity, the productivity of any other employee, or the operation of the City's technical resources. Employees may not play games on the City's computers and other technical resources. Employees may not access non-business-related websites or commercial websites during work time, unless necessary for business purposes and authorized by their direct supervisor.

You must not send e-mail or other communications that either mask your identity or indicate that they were sent by someone else. You may never access any technical resources using another employee's password. Similarly, you may only access the libraries, files, data, programs, and directories that are related to your work duties. Unauthorized review, duplication, dissemination, removal, installation, damage, or

alteration of files, passwords, computer systems or programs, or other property of the City, or improper use of information obtained by unauthorized means, is prohibited.

Sending, saving or viewing obscene material is prohibited at any time. Messages stored and/or transmitted by computer, voicemail, e-mail or telephone systems must not contain content that may reasonably be considered offensive to any employee. Offensive material includes, but is not limited to, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, religion, national origin or ancestry, physical or mental disability, veteran status, as well as any other category protected by federal, state, or local laws. Any use of the Internet/Web, intranet or electronic bulletin board to harass or discriminate is unlawful and strictly prohibited by the City. Violators will be subject to discipline, up to and including discharge.

The City does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the City reserves the right not to provide a defense or pay damages assessed against employees for conduct in violation of this policy.

5. Access to Information

The City asks you to keep in mind that when you are using the City's computers you are creating City documents using a City asset. The City respects the individual privacy of its employees. However, that privacy does not extend to an employee's work-related conduct or to the use of City-provided technical resources or supplies.

The City's computer, voicemail, e-mail or telephone systems, and the data stored on them are and remain at all times the property of the City. As a result, computer data, voicemail messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the City's computer system and other technical resources, your work may be subject to the investigation, search and review of others in accordance with this policy.

All information, including e-mail messages and files, that is created, sent or retrieved over the City's technical resources is the property of the City, and should not be considered private or confidential. Employees have no right to privacy as to any information or file transmitted or stored through the City's computer, voicemail, e-mail or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests and obligations of the City. Employees should also be aware that even when a file or message is erased or a visit to an Internet or website is closed, it is still possible to recreate the message or locate the website. The City reserves the right to monitor your use of its technical resources at any time. All information, including text and images, may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

6. Confidential Information

E-mail and Internet/Web access are not entirely secure. Others outside the City may also be able to monitor your e-mail and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which City, and even which particular person, accessed the service. If your work using these resources requires a higher level of security, please see your supervisor for guidance on securely exchanging e-mail or gathering information from sources such as the Internet or World Wide Web.

All employees should safeguard the City's confidential information, as well as that of citizens and others, from disclosure. Do not access new voicemail or e-mail messages with others present. Messages containing confidential information must not be left visible while you are away from your work area.

E-mail messages containing confidential information must include the following statement, in all capital letters, at the top of the message: CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED. All e-mail messages must use a disclaimer which indicates that confidential information must be maintained appropriately.

7. Security of Information

Although you may have passwords to access computer, voicemail and e-mail systems, these technical resources belong to the City, are to be accessible at all times by the City, and are subject to inspection by the City with or without notice. The City may override any applicable passwords or codes to inspect, investigate or search an employee's files and messages. All passwords must be provided to the City Clerk and made available to your supervisor or other City official upon request. You must not provide a password to other employees or to anyone outside the City and must never access any technical resources using another employee's password.

In order to facilitate the City's access to information on its technical resources, you may not encrypt or encode any voicemail or e-mail communication or any other files or data stored or exchanged on City systems without the express prior written permission from your supervisor. As part of this approval, your supervisor will indicate a procedure for you to deposit any password, encryption key or code, or software with him or her so that the encrypted or encoded information can be accessed in your absence.

8. Copyrighted Materials

You must not copy or distribute copyrighted material *(e.g.*, software, database files, documentation, articles, graphics files and downloaded information) through the e-mail system or by any other means unless you have confirmed in advance from appropriate sources that the City has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the City as well as legal action by the copyright owner. The City will not provide a legal defense to any employee who violates

applicable copyright law. Any questions concerning these rights should be directed to your supervisor.

9. The City's Software Policy

If you want to install software on City computers, you must contact your supervisor and request to have the software installed. Employees are prohibited from installing any software on any City technical resource without the express prior permission from a City official.

Involving a City official ensures that the City can manage the software on City systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the City and the individual employee to substantial fines and exposes the individual employee to imprisonment. Therefore, employees may not load personal software onto the City's computer system and may not copy software from the City for personal use without prior approval from a City official.

The City will cooperate with the copyright holder and legal officials in all copyright matters.

10. Your Responsibilities

Employees are responsible for the content of all text, audio, or images that are placed or sent over the City's technical resources. Employees may access only files or programs, whether computerized or not, that they have permission to enter.

Violations of any guidelines in this policy may result in disciplinary action, up to and including discharge. In addition, the City may advise appropriate legal officials of any illegal violations and cooperate in investigations conducted by legal officials.

Q. Social Media

The City recognizes that many employees choose to participate in social media (i.e. blogs, Twitter, or online forums such as LinkedIn, Facebook, YouTube, and MySpace) in their personal time. Employee participation in social media is voluntary and is not a condition of employment with the City. It is important for employees who choose to use social media to understand what the City recommends, expects, and requires when they discuss City-related topics or identify themselves as City employees online.

1. Employees are personally responsible for the content published on blogs, wikis, or any other form of user-generated media. In addition, employees remain personally responsible for their posts, regardless of whether posted or published on websites owned, operated, or affiliated with the City, or websites that are not affiliated in any way with the City.

2. Do not use ethnic slurs, discriminatory, harassing, threatening, or obscene language, other similarly unacceptable language, or any defamatory, slanderous, or libelous content.

3. Understand and make it clear that you are speaking for yourself and not on behalf of the City. Use a disclaimer such as, "The postings on this site are my own and do not necessarily represent the City's positions, strategies, or opinions."

4. Respect trademark, copyright, and fair use laws.

5. Do not create websites or pages on behalf of specific City offices, departments, etc., unless previously approved by management.

6. Do not communicate the City's confidential and proprietary information, or other information protected from disclosure by the law, applicable contracts, or City policy.

7. Privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the City. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't say it at work or in front of the public, consider whether you should post it online. If you are unsure about posting something or responding to a comment, ask your supervisor for input.

8. Be aware that a presence in the social media world is or easily can be made available to the public at large. Consider this before publishing a post.

9. Do not use the City's resources to engage in online communications unless specifically approved by management in advance for work related purposes.

10. Get the facts straight before posting them on social media. Review content for grammatical and spelling errors. This is especially important if posting on behalf of the City in any capacity.

11. Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of the potential for negative consequences.

12. Remember to follow other general City policies. What you post on social media may be treated like any other communication.

This policy applies to all employees. This policy likewise applies to the use of any social media in the workplace, at home, offsite, and at any other location for business or for personal use.