Section 1: **Purpose**

Since inappropriate use of City systems exposes the City to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of City Information Technology (IT) resources for the protection of all parties involved. Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the City network. This policy explains how City IT resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus, the user is asked additionally to use common sense when using City resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

Section 2: **Scope**

The scope of this policy includes any and all use of City IT resources, including but not limited to, computer systems, email, the network and the City's Internet connection.

Section 3: **Policy**

1. **Email Use**

   Personal usage of City email systems is permitted as long as A) such usage does not negatively impact the City computer network, and B) such usage does not negatively impact the user's job performance.

   • The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

   • The user is prohibited from forging email header information or attempting to impersonate another person.

   • Email is an insecure method of communication, and thus, information that is considered confidential or proprietary to the City may not be sent via email, regardless of the recipient, without proper encryption.

   • It is City policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and, as such, emails should not contain attachments of excessive file size.

2. Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of the City, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

3. Network Access

The user should take reasonable efforts to avoid accessing network data, file, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4. Unacceptable Use

The following actions shall constitute unacceptable use of the City network. This list is not exhaustive, but is included to provide a reference for types of activities that are deemed unacceptable. The user may not use the City network and/or systems to:

- Engage in activity that is illegal under local, state, federal or international law.

- Engage in any activities that may cause embarrassment, loss of reputation or other harm to the City.

- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

- Engage in activities that cause an invasion of privacy.

- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

- Make fraudulent offers for products or services.

- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information-gathering techniques when not part of employee's job function.

- Install or distribute unlicensed or "pirated" software.

• Reveal personal or network passwords to others, including family, friend, or other members of the household when working from home or remote locations.

5. **Blogging**

Blogging by an employee is subject to the terms of this policy, whether performed from the City network or from a personal system. Blogging is only allowed from the City computer network in the conduct of official City business. In no blog shall material detrimental to the City be published. Unless posting to an official City blog, the user must not identify himself or herself as an employee of the City. The user assumes all risks associated with blogging.

6. **Instant Messaging**

Instant Messaging is not permitted on the City network for any purpose.

7. **Overuse**

Actions detrimental to the computer network or other City resources, or that negatively affect job performance are not permitted.

8. **Web Browsing**

The Internet is a network of interconnected computers of which the City has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit or inappropriate. The user must use the Internet at his or her own risk. The City is specifically not responsible for any information that the user views, reads or downloads from the Internet.

Personal Use. The City recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of City computer systems to access the Internet is permitted, as long as such usage follows pertinent guidelines elsewhere in this document, and does not have a detrimental effect on the City or on the user's job performance.

9. **Copyright Infringement**

The City's computer systems and networks must not be used to download, upload or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies or other copyrighted material using Peer-to-Peer (P2P) file sharing or unlicensed CDs and DVDs; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files that the employee has not already legally procured. This list is not meant to be exhaustive. Copyright law applies to a wide variety of works and applies to much more than is listed above.

10. **Peer-to-Peer File Sharing**
    Peer-to-Peer (P2P) networking is not allowed on the City network under any circumstance.

11. **Streaming Media**
    Streaming media can use a great deal of network resources and, thus, must be used carefully. Streaming media is allowed for job-related functions only.

12. **Monitoring and Privacy**
    Users should expect no privacy when using the City network or City resources. Such use may include, but is not limited to: transmission and storage of files, data and messages. The City reserves the right to monitor any and all use of the computer network. To ensure compliance with City policies, this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks and removable media.

13. **Bandwidth Usage**
    Excessive use of City bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low Citywide usage.

14. **Personal Usage**
    Personal usage of City computer systems is permitted during lunch, breaks and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the City or on the user's job performance.

15. **Remote Desktop Access**
    Use of non-City-supplied remote desktop software and/or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited.

16. **Circumvention of Security**
    Using City-owned or City-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

17. **Use for Illegal Activities**
    No City-owned or City-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to, or escalate privileges on, a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing or distributing violent, perverse, obscene, lewd or offensive material as deemed by applicable statutes
- Downloading, storing or distributing copyrighted material

The City will take all necessary steps to report and prosecute any violations of this policy.

18. **Non-City-Owned Equipment**
Non-City-provided equipment is expressly prohibited on the City's network.

19. **Personal Storage Media**
The City does not restrict the use personal storage media, which includes but is not limited to: USB or flash drives, and CD/DVD writers, on the City network, provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware and other undesirable security risks are not introduced onto the City network. Use of personal storage media must conform to the City's Mobile Device Policy.

20. **Software Installation**
Installation of non-City-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

21. **Reporting of Security Incident**

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the City Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains City information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact the City's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

22. **Applicability of Other Policies**

This document is part of the City's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as needed.

Section 4: Enforcement

This policy will be enforced by the IT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more-severe penalties up to and including termination of employment. Where illegal activities are suspected, the City will report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

Section 6: Definitions

Blogging: The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging: A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing: A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access: Remote-control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media: Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.