INFORMATION TECHNOLOGY POLICY

703 – PUBLIC INTERNET Policy

Policy Title:	**PUBLIC INTERNET POLICY**	Policy Number: APR 703
Effective:	November 1, 2012	
Supersedes:	APR #414 dated 11/97	
Approval:		Page 1 of 5

1. Scope

☒ Full-time
☒ Part-time
☒ Temporary/Contract
☒ Salaried
☒ Union
☒ Independent Contractors
☒ Visitors and Vendors
☒ Volunteers/Unpaid Interns

Employees who are covered under the provisions of a collective bargaining agreement will follow the standards as contained in their respective contracts if this policy conflicts with the language in the contract.

This policy is applicable City-wide. All users of City computer and technology resources are expected to comply with this policy as a condition of continued employment or contracted services.

The provisions of this Policy are subject to, and may be superseded by (in the event of a conflict), relevant provisions of applicable collective bargaining agreements between the City and the various collective bargaining associations of the City

2. Purpose

The purpose of this policy is to ensure the appropriate use of the Public Internet and to protect the integrity and availability of City networks.

2.1 Rationale

The Public Internet is an open communication network that serves billions of users worldwide. The Public Internet facilitates business transactions, communication with the public, and provides resources to conduct research. As such, the power of the Public Internet can be harnessed to provide

significant benefits for City business. Conversely, it can present a number of risks if not sufficiently controlled. These risks include breach of security, damage to reputation, lost productivity, legal liability, damage to systems and data, increasing network traffic, etc.

Users must evaluate the importance and sensitivity of any data to be transmitted via the Public Internet, including electronic communications. The objective of this policy is to mitigate risks by ensuring users are aware of their obligations when using the Public Internet via the City's computing systems.

3. Responsibilities

3.1 All users are responsible for:

- Being familiar with and fully complying with this policy
- Ensuring that City information is protected per IT policy requirements (*the City does not automatically protect information sent via the Public Internet*)

3.2 Failure to comply with this policy is a violation of the City's Employee Standards of Conduct policy and may lead to:

- Revocation of system privileges
- Disciplinary action according to the City's Progressive Discipline policy

3.3 Failure to comply with this policy by a contractor using City technology resources may be considered grounds for breach of its contract and revocation of system privileges.

4. Policy

Access to the Public Internet is provided for use by City employees (and other authorized personnel) for legitimate City business purposes.

4.1 Accountability & User Identity

- Users are accountable for their actions when accessing the Public Internet using the City network and/or with City computing resources.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Public Internet or any City electronic communications system is prohibited.
- The use of anonymous proxies or other anonymous facilities are not permitted.

4.2 External Site Access

- The ability to access a specific Public Internet website does not in itself imply that users of City systems are permitted to visit that site. The City

may, at its discretion, restrict or block access to Public Internet sites and/or services and prevent the downloading of certain file types.

4.3 Public Internet Connections

- All communications between a City network and any non-City network must use solutions approved by ITSU management and use network suppliers chosen by the City.
- Service Units are prohibited from procuring unapproved dedicated connections to the Public Internet without the documented approval of ITSU management.
- All communications between City-owned equipment on City premises and any other non-City network (such as the Public Internet) must use solutions approved by ITSU management, which are secured with appropriate administrative and technical controls.

4.4 Appropriate Use of City-provided Public Internet access

4.4.1 City requirements for the appropriate use of City-provided Public Internet access.

- The City is not responsible for the content that users may encounter when they use the Public Internet.
- Users who discover they have connected with a website that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.
- Privileged and confidential City information must only be revealed on the Internet if the information has been officially approved for public release per the City's Communications Guidelines.

4.4.2 Improper use of the Public Internet, City Intranet, electronic communications, and other Public Internet services is prohibited. Improper use includes but is not limited to:

- Accessing, reproducing, downloading, transmitting or possessing any materials that are sexually explicit, obscene, defamatory, harassing, illegal, or otherwise inappropriate
- Accessing, creating, downloading, transmitting or possessing offensive, defamatory, threatening or abusive messages in any way, including through the Public Internet
- Transmitting 'jokes' of an offensive nature, for example, content which is sexually explicit, racially offensive or otherwise demeans people on the basis of their religion, disability, sexual orientation or any other protected attribute

4.5 Privacy and Legal Rights

- The City reserves the right to conduct random audits of its technology resources to identify non-compliance with policies and to monitor or access files, Public Internet usage history, and the contents of electronic communications including but not limited to: email, instant messaging (IM), and text messaging sent through or stored on City technology resources.
- Employees (and other authorized personnel) do not and should not have any expectation of privacy in their use of City-owned technology resources or the contents of any electronic communication or file, both business and personal, sent through or stored on City technology resources.
- Technical support personnel are prohibited from reviewing the content of an individual user's electronic communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Written approval from the City Administrator, City Attorney, Chief Judge, a Service Area Administrator, and/or the Human Resource Director is required prior to any monitoring or review of electronic communications.
- Intellectual Property Rights, such as copyrights, patents, and trademarks must be respected. Users using City Public Internet systems must repost or reproduce material only after obtaining permission from the source or quote material from other sources only if these other sources are properly identified.

4.6 Encryption

- Confidential personal information and information that can be used to gain access to goods, services, or computer resources must not be sent over the Public Internet in readable form. Proper encryption must be used. This type of information includes credit card numbers, Social Security numbers, driver's license numbers, logon passwords, etc.
- Protection mechanisms such as secure Internet connections (https://) or other City-approved encryption techniques can be used to protect sensitive information. Contact ITSU if assistance is needed to determine proper protection methods for sensitive information.
- Whenever encryption is implemented, City-approved encryption methods must be used. The use of all other encryption methods is not permitted.

4.7 Virus Checking

- All files downloaded from City or non-City sources, such as the Public Internet, will be automatically scanned with current ITSU-supplied virus detection software.

4.8 Public Internet Services

- The use of any Public Internet (AKA "Cloud") service must be reviewed and approved by ITSU management. The risk associated with the service must be identified and appropriate controls to minimize the risk must be defined and implemented. An ITSU staff member must be included in the development of any business case and process.
- Use of a Public Internet service for other than its intended purpose is considered an abuse of the service and is subject to termination of the right to use the service.

4.9 Management Review

- At any time and without prior notice, City management reserves the right to examine electronic messages, files stored on City-owned technology resources, web browser history/cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through City systems.