Section 1: Purpose

This policy is provided to define standards for accessing City Information Technology (IT) resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium. It is often necessary to provide access to City information resources to employees or others working outside the City's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

Section 2: Scope

The scope of this policy covers all employees, contractors and external parties who access City resources over a third-party network, whether such access is performed with City-provided or non-City-provided equipment.

Section 3: Policy

1. Prohibited Actions

Remote access to City systems is only to be offered through a City-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router or other remote-access device on a City system without the approval of the IT Manager.
- Remotely accessing City systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the IT Manager.
- Use of non-City-provided remote access software.
- Split Tunneling to connect to an insecure network in addition to the City network, or in order to bypass security restrictions.

2. Use of non-City-provided Machines

Accessing the City network through home or public machines can present a security risk, as the City cannot completely control the security of the system accessing the network. Use of non-City-provided machines to access the City network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed

- Its software patch levels are current
- It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

3. **Client Software**
The City will supply users with remote access software or a secure connection means that allows for secure access and enforces the remote access policy. This will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

4. **Network Access**
There are no restrictions on what information or network segments users can access when working remotely; however, the level of access should not exceed the access a user receives when working in the office.

5. **Idle Connections**
Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the City's network must be timed out after 1 hour of inactivity.

6. **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.

Section 5: Definitions

Modem: A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access: The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email or other resources at a main site.

Split Tunneling: A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout: A technique that drops or closes a connection after a certain period of inactivity.

Two-Factor Authentication: A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens or biometrics, in combination with a password.