# Section 1: **Purpose**

The purpose of this policy is to state the standards for wireless access to the City's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the City wishes to take to secure its wireless infrastructure. Wireless communication is playing an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

# Section 2: **Scope**

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards and anything else capable of transmitting or receiving a wireless signal.

# Section 3: **Policy**

## 1. Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas must be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points should be secured so that it cannot be accessed without difficulty.

## 2. Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

### a. Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify the City, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the City.

• Encryption must be used to secure wireless communications. Stronger algorithms are preferred to weaker ones (i.e., WPA should be implemented rather than WEP). Encryption keys must be changed and redistributed quarterly.

• Administrative access to wireless access points must utilize strong passwords.

• All logging features should be enabled on the City's access points.

b. **Installation**

• Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.

• Wireless networking must not be deployed in a manner that will circumvent the City's security controls.

• Wireless devices must be installed only by the City's Information Technology (IT) Division.

• Channels used by wireless devices should be evaluated to ensure that they do not interfere with City equipment.

## 3. Accessing Confidential Data

If confidential data is to be accessed over the wireless network, additional security measures must be taken since the security of the wireless LAN cannot be absolutely verified. The City's remote access policy must be followed in order to provide additional encryption software (IPSec, SSL, etc.) to secure this data during wireless transmission.

## 4. Inactivity

Users should disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.

Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the City.

## 5. Audits

The wireless network must be audited twice each year to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, and use of strong encryption.

## 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 sever- penalties up to and including termination of employment.

## Section 5: **Definitions**

**Mac Address:** Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

**SSID:** Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

**WEP:** Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

**WiFi:** Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

**Wireless Access Point:** A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

**Wireless NIC:** A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

**WPA:** Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.