Section 1: **Purpose**

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the City network are authenticated in an appropriate manner, in compliance with City standards, and are given the least amount of access required to perform their job function. Any user accessing the City's computer systems has the ability to affect the security of all users of the system. A sound network access policy provides consistent application of authentication and access standards across the City.

Section 2: **Scope**

The scope of this policy includes all users who have access to City-owned or City-provided computers or require access to the City network and/or systems.

Section 3: **Policy**

1. **Account Setup**
   During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

   - Positive ID and coordination with Administrative Services is required.

   - Users will be granted the least amount of network access required to perform his or her job function.

   - Users will be granted access only if he or she accepts the Acceptable Use Policy.

   - Access to the network will be granted in accordance with the Acceptable Use Policy.

2. **Account Use**
   Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

   - Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)

   - Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

- Occasionally, guests will have a legitimate business need for access to the City network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources the guest needs at that time, and disabled when the guest's work is completed.

3. **Account Termination**
When managing network and user accounts, it is important to stay in communication with the Administrative Services Department so that when an employee no longer works at the City, that employee's account can be disabled. Administrative Services must create a process to notify the Information Technology (IT) Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4. **Authentication**
User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

5. **Use of Passwords**
When accessing the network locally, username and password is an acceptable means of authentication.

6. **Remote Network Access**
Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the City encourages additional scrutiny of users allowed to remotely access the network. The City's standards dictate that username and password is an acceptable means of authentication. Remote access must adhere to the Remote Access Policy.

7. **Screensaver Passwords**
Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are required

to be activated after 15 minutes of inactivity.

8. **Minimum Configuration for Access**
   The IT Division will update users' antivirus software, as well as other critical software, to the latest versions before accessing the network.

9. **Encryption**
   Authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the City network or across a public network such as the Internet.

10. **Failed Logons**
    Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the City must lock a user's account after 10 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

    In order to protect against account guessing, when logon failures occur, the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

11. **Non-Business Hours**
    While some security can be gained by removing account access capabilities during non-business hours, the City does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the City's business requires all-hours access.

12. **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 an, 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, and should be validated through periodic audit. 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**

Antivirus Software: An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware and other malware.

Authentication: A security method used to verify the identity of a user and authorize access to a system or network.

Biometrics: The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns and hand geometry.

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Password: A sequence of characters that is used to authenticate a user to a file, compute, or network. Also known as a passphrase or passcode.

Smart Card: A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Token: A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.