Section 1: **Purpose**

The purpose of this policy is to outline the City's standards for use of encryption technology so that it is used securely and managed appropriately. Many policies touch on encryption of data, so this policy does not cover what data is to be encrypted, but rather how encryption is to be implemented and controlled. Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data the City must store digitally increases, the use of encryption must be defined and consistently implemented in order to ensure that the security potential of this technology is realized.

Section 2: **Scope**

This policy covers all data stored on or transmitted across City systems.

Section 3: **Policy**

1. Applicability of Encryption

a. Data while stored. This includes any data located on City-owned or City-provided systems, devices, media, etc. Examples of encryption options for stored data include:

- Whole-disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications

b. Data while transmitted. This includes any data sent across the City network, or any data sent to or from a City-owned or City-provided system. Types of transmitted data that can be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments

- Remote desktop access
- Communications with applications/databases

2. **Encryption Key Management**

Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to the City's encryption keys and key management:

- Management of keys must ensure that data is available for decryption when needed
- Keys must be backed up
- Keys must be locked up
- Keys must never be transmitted in clear text
- Keys are confidential data
- Keys must not be shared
- Physical key generation materials must be destroyed within 5 business days.
- Keys must be used and changed in accordance with the password policy.
- When user encryption is employed, minimum key length is 10 characters.

3. **Acceptable Encryption Algorithms**

Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, such as AES or 3DES. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured.

4. **Legal Use**

Some governments have regulations applying to the use and import/export of encryption technology. The City must conform with encryption regulations of the local or applicable government.

The City specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

5. **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 Information Technology (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.

Section 5: Definitions

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.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.

Mobile Storage Media: A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive or thumb drive.

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.

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.

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.

Virtual Private Network (VPN): A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

Whole Disk Encryption: A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.