Section 1: **Purpose**

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified. Information assets are assets to the City just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to City operations and the confidentiality of its contents. Once this has been determined, the City can take steps to ensure that data is treated appropriately.

Section 2: **Scope**

The scope of this policy covers all City data stored on City-owned, City-leased, and otherwise City-provided systems and media, regardless of location. Also covered by the policy are hardcopies of City data, such as printouts, faxes, notes, etc.

Section 3: **Policy**

1. Data Classification

Data residing on City systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. Public: includes already-released material, commonly known information, etc. There are no requirements for public information.

3. Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more-detailed information about how to handle confidential data.

2. Data Storage

The following guidelines apply to storage of the different types of City data.

a. Personal

There are no requirements for personal information.

b. Public

There are no requirements for public information.

c. **Operational**
Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

d. **Critical**
Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

e. **Confidential**
Confidential information must be removed from desks, computer screens and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured.

3. Data Transmission

The following guidelines apply to transmission of the different types of City data.

a. **Personal**
There are no requirements for personal information.

b. **Public**
There are no requirements for public information.

c. **Operational**
No specific requirements apply to transmission of Operational Data; however, as a general rule, the data should not be transmitted unless necessary for business purposes.

d. **Critical**
There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

e. **Confidential**
Confidential data must not be 1) transmitted outside the City network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the City's network.

4. Data Destruction

The following guidelines apply to the destruction of the different types of City data.

a. **Personal**
There are no requirements for personal information.

b. **Public**
There are no requirements for public information.

c. **Operational**
Cross-cut shredding is required for documents. Storage media should be appropriately sanitized/wiped or destroyed.

d. **Critical**
There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

e. **Confidential**
Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross-cut shredding is required.
- Storage media (CDs, DVDs): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the City must follow U.S. DoD standards for data wiping. Alternatively, the City has the option of physically destroying the storage media.

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 or theft of City property (physical or intellectual) are suspected, the City will report such activities to the applicable authorities.

Section 5: Definitions

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

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

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.

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

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.

U.S. DoD Standards: Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22-M. Most data-wiping software packages provide an option for wiping to this standard.