Section 1: **Purpose**

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed. A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A City's backup policy is among its most important policies.

Section 2: **Scope**

This policy applies to all data stored on City systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups and restoration procedures.

Section 3: **Policy**

1. Identification of Critical Data

The City must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

2. Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources and the backup administrator. Data to be backed up will include:

- All data determined to be critical to City operation and/or employee job function.

- All information stored on the City file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.

- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls and remote access servers, etc.

3. **Backup Frequency**

Backup frequency is critical to successful data recovery. The City has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network and backup administrator.

Incremental: every day
Full: every week

4. **Off-Site Rotation**

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the City's uptime requirements. The City has determined that backup media must be rotated off-site at least once per week.

5. **Backup Storage**

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, City data, precautions must be taken that are commensurate to the type of data being stored. The City has set the following guidelines for backup storage.

When stored onsite, backups should be kept in an access-controlled area. When shipped off-site, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. Online backups are allowable if the service meets the criteria specified herein.

6. **Backup Retention**

When determining the time required for backup retention, the City must determine what number of stored copies of backup data is sufficient to effectively mitigate risk while preserving required data. The City has determined that the following will meet all requirements (note that the backup retention policy must conform to the City's data retention policy and any industry regulations, if applicable):

Incremental Backups must be saved for one month.
Full Backups must be saved for six months.

7. **Restoration Procedures & Documentation**

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request

to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

8. **Restoration Testing**
   Since a backup policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems.

   Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year.

9. **Expiration of Backup Media**
   Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service, the media can no longer be considered dependable. When backup media is put into service, the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

10. **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

The backup policy will be enforced by the designated backup administrator, the IT Manager, and/or the executive team, and should be validated through periodic audit. Violations may result in disciplinary action, which may include suspension or more-severe penalties up to and including termination of employment.

Section 5: Definitions

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

Backup Media: Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Backup: A backup that makes a complete copy of the target data.

Incremental Backup: A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

Restoration: Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.