Section 1: Purpose

The purpose of this policy is to specify actions to take when selecting a provider of outsourced Information Technology (IT) services, standards for secure communications with the provider, and what contractual terms should be in place to protect the City. Outsourcing is a logical practice when specialized expertise is required, which happens frequently in the field of IT. Trust is necessary for a successful outsourcing relationship; however, the City must be protected by a policy that details and enforces the terms of the outsourcing relationship.

Section 2: Scope

This policy covers any IT services being considered for outsourcing.

Section 3: Policy

1. Deciding to Outsource

Outsourcing IT services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered:

- Can the service be performed better or less expensively by a third-party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?

2. Outsourcing Core Functions

The City permits the outsourcing of critical and/or core functions of the City's Information Technology infrastructure as long as this policy is followed. Examples of these types of functions are data backups, remote access, security, and network management.

3. Evaluating a Provider

Once the decision to outsource an Information Technology function has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected.

Due diligence should include an evaluation of the provider's ability to perform the requested services, and must specifically cover the following areas:

- Technical ability of the provider
- Ability to deliver the service
- Experience of the provider
- Reputation of the provider
- Policies and procedures related to the service
- Financial strength of the provider
- Service Level Agreements related to the service

If the outsourced service will involve the provider having access to, or storing the City's confidential information, due diligence must cover the provider's security controls for access to the confidential information.

4. Security Controls

The outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

The City and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to City data.

5. Outsourcing Contracts

All outsourced IT services must be governed by a legal contract, with an original of the executed contract maintained by the City.

Contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels

- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Describe how and where to handle contractual disputes

6. **Access to Information**
   The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.

7. **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 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.

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.

Network Management: A far-reaching term that refers to the process of maintaining and administering a network to ensure its availability, performance and security.

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.

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