Section 1: Purpose

The policy is intended to provide guidelines for deploying and securing direct connections to third parties. Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery. Since the City's security policies and controls do not extend to the users of the third-parties' networks, these connections can present a significant risk to the network and thus, require careful consideration.

Section 2: Scope

The scope of this policy covers all direct connections to the City's network from non-City owned networks. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

Section 3: Policy

1. **Use of Third-Party Connections**
   Third-party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third-party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the Information Technology (IT) Manager.

2. **Security of Third-Party Access**
   Third-party connections require additional scrutiny. The following statements will govern these connections:

   • Connections to third parties must use a firewall or Access Control List (ACL) to separate the City's network from the third party's network.

   • Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.

   • Wherever possible, systems requiring third-party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.

   • If a third-party connection is deemed to be a serious security risk, the IT Manager will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the IT

Manager.

3. **Restricting Third-Party Access**
Best practices for a third-party connection require that the link be held to higher security standards than an intra-City connection. As such, the third party must agree to:

- Restrict access to the City's network to only those users who have a legitimate business need for access.

- Supply the City with on-hours and off-hours contact information for the person or persons responsible for the connection.

- (If confidential data is involved) Provide the City with the names and any other requested information about individuals that will have access to the City's confidential data. The steward or owner of the confidential data will have the right to approve or deny this access.

4. **Auditing of Connections**
In order to ensure that third-party connections are in compliance with this policy, they must be audited periodically.

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 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

Access Control List (ACL): A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Demilitarized Zone (DMZ): A perimeter network, typically inside the firewall but external to the private or protected network, where publicly accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

Firewall: A security system that secures the network by enforcing boundaries between

secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Third-Party Connection: A direct connection to a party external to the City. Examples of third-party connections include connections to customers, vendors, partners or suppliers.