BTS-2.16 - Firewall Security & Management

FIREWALL SECURITY & MANAGEMENT
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.16

Purpose
This policy describes the methods and responsibilities for securing the City network, resources and information. Specifically, this policy outlines the standards and authority for managing the City's perimeter defense equipment known as firewalls.

Administrative Rule
The Information Security Office is responsible for developing all policies, standards and configurations for the implementation and use of firewalls within the City. These policies and standards include but are not limited to:

- A stateful packet inspection firewall is required at each Internet connection.
- A stateful packet inspection firewall is required between any Demilitarized Zone (DMZ) and the City's network resources
- A stateful packet inspection firewall shall reside between the Internet and any City system, resource or network-connected or device. Inbound internet traffic shall be limited to DMZs that include systems which provide authorized publicly accessible services, protocols and ports.

Intrusion detection or prevention technology shall be implemented at network perimeters and critical network access points, and where deemed necessary for compliance, and shall alert appropriate personnel to suspicious network events or malicious behavior.

Written justification is required to provide a connection through a firewall. Business Systems Owners shall submit written documentation for all access changes required to conduct their business. Submitted documentation shall include the business reasons for these changes and the end date for this business need.

The Information Security Office approves any requests for additional protocols. BTS firewall administrators evaluate any requests for additional protocols and maintain all documentation on the business need for these protocols. All protocols from external and/or untrusted networks are not permitted without this written justification. Firewalls shall be configured to specifically deny traffic that has not been approved and documented.

Firewall rules shall be reviewed by BTS firewall administrators at least once every six months to ensure the rules accuracy and continued necessity.

History
Adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.
Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.
This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.
This rule was reviewed as part of a periodic review and remains unchanged. April 30, 2018.