BTS-2.16 - Firewall Security and Management

FIREWALL SECURITY AND 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 internal network and data. 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 internal network
- A stateful packet inspection firewall shall reside between the Internet and any City system or device.

Written justification is required to provide a connection through a firewall for any protocols other than HTTP, HTTPS, and SSH. Data owners shall submit written documentation for any other network protocols needed to conduct their business. This documentation shall include the business reasons for these protocols and the end date for this business need. The Information Security Office approves any requests for additional protocols and maintains all documentation on the business need for these protocols. All protocols from external and/or untrusted networks are not permitted without this written justification.

Firewall rules shall be reviewed by the Information Security Office 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.