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 City Trusted Networks, City Technology Resources, and City Confidential and Restricted Information. Specifically, this policy outlines the standards and authority for managing the City's Trusted Networks and cybersecurity threat detection, prevention and defense systems collectively known as firewalls.

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

1. A stateful packet inspection firewall is required at each Internet and external data interfacing connection.
2. A stateful packet inspection firewall is required between any Demilitarized Zone (DMZ) and the City's Trusted Networks and City Technology Resources.
3. A stateful packet inspection firewall must reside between the Internet and any City system, resource or network-connected device. Inbound Internet traffic must be limited to DMZs that include security systems and capabilities which provide authorized publicly accessible services, protocols and data ports.
4. Determination of Standard Changes and Risk Assessments for firewall rule additions, change, and exceptions.
    a. Additional Firewall Standards are defined within the City of Portland Information Security Standards document
5. Firewalls must be configured to specifically deny traffic that has not been approved and documented.6. Firewall rules must be reviewed by BTS firewall administrators at least once every six months to ensure the rules' accuracy and continued necessity.

Intrusion Detection and Prevention
Intrusion Detection and Prevention Systems (IPS/IDS) must be implemented at network perimeters and critical network access points, and where deemed necessary for compliance, and must alert appropriate BTS Support Professionals and BTS Support Staff to suspicious network activities, incidents or malicious behavior.

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

1. The Information Security Office approves or denies all requests to modify the City's cybersecurity posture and for allowing additional protocols, services and access to City Technology Resources.
2. BTS firewall administrators evaluate all requests for firewall rule changes and maintains all required documentation on the business need for the firewall rules.
3. Requests for additional firewall rule and protocol changes from external and/or untrusted networks are not permitted without written justification from Business Systems Owners and approval from the Information Security Office.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

1) BTS Technology Definitions – https://www.portlandoregon.gov/citycode/article/114449
2) (BTS) Technology Standards Directory (and Acronyms) -- https://www.portlandoregon.gov/bts/article/44978
3) City of Portland Information Security Standards

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.
This rule was reviewed and revised as part of a periodic review. September 2, 2019.
This rule was reviewed and revised as part of a periodic review. June 30, 2020.
This rule was reviewed as part of a periodic review. September 1, 2021.