BTS-2.10 - Wireless 802.11 Networks

WIRELESS 802.11 NETWORKS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.10

Purpose
This policy prohibits access to City networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or those which have been granted an exclusive waiver by the CTO or the Information Security Manager (ISM) are approved for connectivity to the City's networks.

This policy covers all 802.11 wireless data communication devices (e.g., personal computers, laptops, notebooks, Smartphones, tablet computers, etc.) which connect to any of the City's internal networks or systems.

Administrative Rule

Register Wireless Devices: All wireless devices (Access Points, Base Stations and Network Interface Cards) connected to the City network must be approved, registered, installed and maintained by the Bureau of Technology Services (BTS).

Encryption and Authentication: To connect to the City network, all computers with wireless LAN devices must utilize a City approved configuration which drops all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point-to-point hardware encryption of at least 128- bits. All implementations must support a hardware address (MAC address) that can be registered and tracked. All wireless implementations must support and employ strong user authentication which checks against a BTS approved and managed RADIUS database and support 802.1x authentication.

Setting the SSID: All wireless access points shall have their SSID configured so that it either is not broadcast or does not contain the default supplied by the manufacturer.

Penetration Tests and Audits: Wireless Access Points & Base Stations are subject to periodic penetration tests and audits. Unapproved wireless access points and/or those devices which do not comply with BTS approved security configurations are subject to immediate network disconnection and equipment confiscation.

HISTORY

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.