BTS-2.09 - Portable Computing Devices

PORTABLE COMPUTING DEVICES

Administrative Rule Adopted by Council
ARC-BTS-2.09

Purpose

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop and laptop devices in a wide number of applications. However, the portability and small size offered by these devices may increase the security exposure to organizations using such devices.

The purpose of the City′s Portable Computing Security Policy is to establish the rules for the use of portable computing devices and their connection to the City network. These rules are necessary to preserve the integrity, availability and confidentiality of City information and assets.

This policy covers all portable computing devices (PDA′s, Blackberries, Smart Phones, etc) owned, maintained and operated by the City.

Note: Laptop and notebook computers do not apply to this policy, however they are covered under all the same policies applicable to desktop computers & workstations.

Administrative Rule

• Only BTS approved portable computing devices may be used to access City information systems.

• All portable computing devices must be registered with the BTS Operations group′s asset management system and included asset tags or other identification markings for tracking which are required per City accounting policy. Please note, personal identification markings which could inform a thief of the nature of sensitive material stored on any personal computing device, should be avoided.

• Where technically feasible, all portable computing devices must be password protected and have an inactivity timeout. Any devices with non-public information shall have enabled a lock-out feature to restrict the number of password guesses and comply with all other City password policies or shall use encrypted storage for non-public information.

• All portable computing devices which access the City network (other than synchronization with a City desktop or laptop) must have BTS approved antivirus products and firewalls operational at all times to prevent propagation of malicious code (viruses, trojans, worms, etc.).

• In general, sensitive City data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive City data must be encrypted using BTS approved encryption techniques.

• SensitiveCity data must not be transmitted via wireless to/or from a portable computing device unless BTS approved wireless transmission protocols along with approved encryption techniques are implemented.

• All remote access to the City network must be either through a City approved access gateway or via an Internet Service Provider (ISP).

• Non-City portable computing devices that require network connectivity must conform to City information security policies and standards and must be approved in writing by the CTO or delegate in consultation with the Information Security Manager and Operations Manager.

• AllCity employees must be responsible to secure portable computing devices in their care and possession and immediately report any loss or theft of such devices to their bureau management. Additionally, if such devices support connectivity to the City network, the BTS Helpdesk should be contacted to take immediate steps to protect against unauthorized access to the City's information assets.

Guidelines

• When not in use, external wireless communication mechanisms such as 802.11 or Bluetooth, should be turned off.

• Beware of shoulder surfers. When people peer over your shoulder in the airport or other public places, they may be trying to see confidential data or watch you type in a password. When possible, use a polarizing screen cover which helps prevent viewing the display screen from side angles.

• When conducting City business wirelessly, without VPN technologies, Wi-Fi access points (such as those at coffee shops) should be avoided since they may not have all the proper security features enabled.

History

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.