BTS-2.09 - Portable Computing Devices

PORTABLE COMPUTING DEVICES
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.09

Purpose
Portable computing devices are increasingly powerful and affordable. Their small size and functionality make these devices a desirable replacement for traditional desktop computers in a wide number of applications. However, these devices' portability may increase the security risks to organizations using such devices.

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

This policy covers all portable computing devices (laptops, smartphones, tablet computers, etc.) owned, maintained and operated by the City.

Administrative Rule

- Only BTS approved portable computing devices may be used to access City information systems. The BTS Support Center Manager shall determine the approved devices in consultation with the Chief Information Security Officer (CISO).

- Where technically feasible, portable computing devices 1) shall comply with BTS Administrative Rules including, but not limited to, network access, remote network access, user and administrative passwords and 2) have a BTS approved anti-malware product and personal firewall operational at all times to prevent propagation of malicious software (viruses, trojans, worms, etc.).

- Portable computing devices that cannot support BTS Administrative Rule 2.05 User and Administrative Passwords shall be required at a minimum to implement a four-digit PIN with a fifteen minute inactivity lockout.

- Confidential City data should not be stored on portable computing devices without additional protections. Any portable computing devices with confidential data shall use BTS approved encryption techniques for confidential data storage. Portable computing devices with restricted data are required to use encrypted storage for such information. Please see BTS Administrative Rule 2.18 Information Classification & Protection Policy for more information on the definition of confidential and restricted information.

- Sensitive City 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 comply with BTS Administrative Rule 2.04 Remote Network Access.

- Non-City portable computing devices that require City network connectivity must conform to City information security policies and standards.

- All City 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.

- Exceptions to this Administrative Rule must be approved in writing by the Chief Technology Officer (CTO) or the Chief Information Security Officer (CISO).

Guidelines

- 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, public 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

Ordinance No. 179999, passed by City 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 July 27, 2010.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.
Revised rule adopted by Chief Technology Officer November 15, 2013.
This rule was reviewed as part of a periodic review and remains unchanged, 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. August 20, 2018.