BTS-2.09 - Mobile Computing and Removable Media

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Policy category: Information Security

Policy number: BTS-2.09

Mobile Computing and Removable Media

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority

ARB-BTS-2.09

Search Code, Charter, Policy

Keywords

Search

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.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

BTS-2.09 Mobile Computing and Removable Media Administrative Rule 114.29 KB

BTS-2.09 - Mobile Computing and Removable Media

MOBILE COMPUTING AND REMOVABLE MEDIA
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.09

Purpose
Mobile computing and Removable Media storage devices are increasingly powerful and affordable. Their small size, capacity and functionality make these devices a desirable replacement for traditional desktop computers and enhance information use and transfer in a wide number of applications. However, the portability of these devices increases the City's security risks for loss of City Confidential and Restricted Information. See: https://www.portland.gov/sites/default/files/2020-06/bts-2.18-information-classification-protection-699964.pdf

The purpose of the City's Mobile Computing and Removable Media security Administrative Rule is to establish the rules for the use of mobile computing and Removable Media devices and their connection to the City's networks and authorized Internet-based Service Provider hosted services. These rules are necessary to preserve the integrity, availability and confidentiality of City information and assets.

This policy covers smartphones, laptops, tablets, portable data storage devices, and Removable Media (USB drives, and optical disks) owned, maintained and operated by the City.

Administrative Rule

1. Only Bureau of Technology Services (BTS) approved mobile computing and Removable Media devices may be used to access City information systems and resources. The BTS Support Center Manager determines City-approved devices in consultation with the Senior Information Security Officer (SISO).

2. Employees may not download City information onto personal devices.

3. Where technically feasible, mobile computing devices and Removable Media 1) must comply with BTS Information Security Standards and Administrative Rules including, but not limited to, network access, remote network access, Authorized User and administrative passwords and 2) have BTS approved storage encryption, anti-malware capability, and device firewall (if applicable) operational at all times to prevent propagation of Salacious Software or the loss of City Confidential and Restricted Information.

4. When technical information security controls are not feasible an Information Security Office approved exception is required.

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

6. City Confidential Information stored on mobile computing devices or Removable Media must use BTS approved encryption techniques for temporary data storage. Mobile computing devices and Removable Media with City Confidential and Restricted Information are recommended to use BTS approved encryption techniques for temporary data storage. Please see BTS Administrative Rule 2.18 Information Classification & Protection Policy for more information on the definition of Confidential and Restricted information. BTS 2.18 https://www.portland.gov/policies/technology-services/information-security/bts-218-information-classification-protection

7. City Confidential and Restricted Information must not be transmitted via wireless technology to/or from a mobile computing device unless BTS approved encrypted wireless transmission protocols are implemented. See also *BTS-2.10 - Wireless 802.11 Networks.*

8. All remote and mobile device access to City networks and authorized Internet-based Service Provider hosted services must comply with BTS Administrative Rule *BTS-2.04 Remote Network Access*.

9. Non-City owned mobile computing devices and remote access services that require City network connectivity must conform to City information security policies and standards. Non-City owned or managed mobile devices may have limited access rights to City Technology Resources and information.

10. All City Authorized Users must secure mobile computing devices and Removable Media in their care and possession and immediately report any loss or theft of such devices to their bureau management and BTS HelpDesk. Additionally, if such devices support connectivity to City networks, the BTS Helpdesk must be contacted to take immediate steps to protect against unauthorized access to the City's Technology Resources.

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

Guidelines

1. Always refer to Citywide Information Security awareness resources to protect City Confidential and Restricted Information, and with additional caution when using mobile computing devices, Removable Media, and when remotely accessing City Technology Resources.

2. All wireless connectivity (Wi-Fi) to City Trusted Networks and Technology Resources must use Virtual Private Networks (VPNs) or BTS approved encrypted transmission technologies. City Guest Wi-Fi is not a secure or Trusted Network, does not encrypt transmissions, is not intended for internal City business, and is intended for non-confidential public use within City facilities. See also *BTS-2.10 - Wireless 802.11 Networks.*

References

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

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.
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.