BTS-2.04 - Remote Network Access

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

Policy category: Information Security

Policy number: BTS-2.04

REMOTE NETWORK ACCESS

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

ARB-BTS-2.04

HISTORY

Originally published as PPD number ARC-BIT-2.05, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.

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

Re-indexed by Auditor as PPD number ARC-BTS-2.04.

Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.

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 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. April 30, 2018.

Revised by Chief Technology Officer October 10, 2018.

Related documents

- BTS-2.04 Remote Network Access Administrative Rule (22.08 Kb)

BTS-2.04 - Remote Network Access

REMOTE NETWORK ACCESS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.04

Purpose
Remote network access is a generic term used to describe accessing an organization's computer network by individuals not located at the organization's offices. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home. In many cases, both the organization and the employee may benefit from the increased flexibility provided by remote access. As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the remote access are not fully understood by all participants.

The purpose of this policy is to define the approved method for City employees to remotely connect to the City network and how their connection will be established, controlled and managed.

Administrative Rule
Remote access to the City network by City employees is authorized when business activities require it, subject to approval by Bureau or Office Management. The approved method of remote access is through a Virtual Private Network (VPN) connection.

The following policies apply to those approved for remote VPN access to the City network.

- Remote network access shall only occur via a BTS maintained virtual private network (VPN) system. This does not apply to the use of the City portal applications with secure access support, such as the City's web and/or email portal. Full VPN tunnel access is only available to BTS maintained systems.

- When actively connected to the City network, VPNs force all traffic to and from the remote computer over the VPN tunnel. All other traffic will be dropped. Split tunneling is not permitted; only one network connection is allowed.

- All authorized remote VPN users assume responsibility to assure that unauthorized users do not access City networks through their systems, software or configurations. This includes employee's family members, friends, and associates.

- Since VPN connections offer a private connection into the City's network from the internet, additional security measures are required to prevent unauthorized access, including but not limited to two-factor authentication.

- For non-City employees such as vendors and contractors, the responsible Business System Owner must identify remote network access requirements with proper written justification of the business reasons for such access. Additionally, remote access for vendors or contractors shall only be enabled during the time period needed, disabled when not in use, and promptly deactivated after access is no longer necessary. The Chief Information Security Officer (CISO) shall hold the final approval for all remote access to the City's network.

Exceptions to this policy, or any sections thereof, may be granted on a case-by-case basis by the Chief Technology Officer (CTO) or the Chief Information Security Officer (CISO). If an exception is granted for VPN technology on non-City computers, users acknowledge that their machines are a de facto extension of the City's network and as such, are subject to all the same policies that apply to City employees and City owned and managed equipment, including, but not limited to acceptable minimal security standards of system and software.

Responsibility
The Bureau of Technology Services is responsible for setting up remote VPN access in a manner that is consistent with information security standards and policies. Such standards and policies include

current malware protection software, operating systems, operating systems patches, firewalls as well as other security and remote administration tools.

History

Originally published as PPD number ARC-BIT-2.05, authorized by Ordinance No. 177048, passed by Council and effective November 6, 2002.
Revised by Ordinance No. 179999, passed by Council March 15, 2006 and effective April 14, 2006.
Re-indexed by Auditor as PPD number ARC-BTS-2.04.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.
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 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. April 30, 2018.