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 and approved vendors and contractors, to remotely connect to the City network and how their connection will be established, controlled and managed.

Administrative Rule

City employees, vendors and contractors have the capability to remotely access the City's network. This access may be suspended or terminated based on Bureau or Office management request or BTS determination that remote network access has been misused or has compromised the City's information security. The approved method of remote access is through a Virtual Private Network (VPN) connection.

The following policies apply to utilizing remote VPN access to the City's network:

- When actively connected to the City network, the City's VPN will 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.
- Remote VPN users assume the 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.
- Security measures, such as a patched operating system, a current personal firewall, and current anti-virus software are required to prevent unauthorized access to the City's network. Additional security measures, such as strong authentication technologies, are also required for those users who seek to remotely access internal City network resources.
- For non-City employees such as vendors and contractors, the responsible Bureau Manager must identify and approve remote network access requirements with proper written justification.

Exceptions to this policy, or any sections thereof, may be granted on a case-by-case basis by the CTO or the Information Security Manager. Users who access the City's network via non-City computers understand that their computers 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 computing equipment.

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 virus protection software, operating systems, operating systems patches, firewalls as well as other security and remote administration tools, such as strong authentication technologies. The Information Security Office is responsible for maintaining these technologies; as well as providing policy, procedure, and configuration guidance related to remote network access.

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.