BTS-2.04 - Remote Network Access

REMOTE NETWORK ACCESS
Administrative Rule Adopted by Council
ARC-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.

- Only City-owned and BTS managed computers shall be used for remote network access from the internet. Such access will be via City licensed and standard virtual private network (VPN) systems installed and maintained by the Bureau of Technology Services. This does not apply to the use of the City web portal applications with secure access support, such as www.portlandonline.com and the City's email portal. • When actively connected to the City network, VPN's 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.
- VPN gateways will only be setup and maintained by BTS network operations personnel.
- All authorized remote VPN users, must remain diligent and 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.
- As VPN connections offer a private connection into the City network from the global public internet, additional security measure are required to prevent unauthorized access. As a result, all City VPN users are subject to more stringent password requirements and authentication mechanisms.
- For non-City employees such as vendors and contractors, the responsible Bureau Manager must identify remote network access requirements with proper written justification and receive prior approval from the CTO or delegate in consultation with the Information Security Manager and Operations Manager.
- All requests for remote network access must be made by completing the appropriate

request form. http://www.portlandonline.com/omf/index.cfm?c=39147

Exceptions to this policy, or any sections thereof, may be granted on a case-bycase basis by the CTO or delegate in consultation with the Information Security Manager and BTS Operations Manager. If an exception is granted for VPN technology on non-City computers, users understand 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.

Responsibility

Bureaus or Offices must use the BTS Remote Access Service Request form to notify BTS of individuals who require remote VPN access to the City network. http://www.portlandonline.com/omf/index.cfm?c=39147

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.

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.