BTS-2.04 - Remote Network Access

REMOTE NETWORK ACCESS (Remote City Technology Resources 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 the City's Technology Resources by Authorized Users who are not located within the City's facilities. Remote access may take the form of traveling Authorized Users, Authorized Users who regularly work from home, or Authorized Users who work both from the office and from home. In many cases, both the City and the Authorized User 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.

Internet-based, or "Cloud" computing Software as a Service (SaaS) services that contain City information are included within the scope of Bureau of Technology Services (BTS) Administrative Rules which apply to all City information repositories regardless of their storage locations or means of access.

The purpose of this policy is to define the approved methods for City Authorized Users to remotely connect to and access City Technology Resources and how these connections will be established, controlled and managed.

Administrative Rule
Remote access to City Technology Resources by Authorized Users is authorized when business activities require it, subject to approval by the Chief Technology Officer (CTO), the Senior Information Security Officer (SISO), or their delegate. The approved methods of remote access are through an authorized Virtual Private Network (VPN) connection from a City-managed device, or resource-limited access to the City's Microsoft Office 365 environment (Microsoft e-mail, Microsoft Teams, Microsoft OneDrive, or the Hitachi Anywhere portal.) with Multi-Factor Authentication (MFA).

The following additional policies apply to those Authorized Users approved for remote VPN access to City Technology Resources.

1. Remote network access must only occur via a BTS maintained and authorized virtual private network (VPN) system. A VPN is not required to the use of the City portal applications with secure access support, such as the City's web and Microsoft Office 365 portal. Full VPN tunnel access is only available to BTS maintained devices.

2. When actively connected to City Technology Resources, VPNs force all traffic to and from the remote device through the VPN tunnel. All other traffic is blocked unless City

defined split-tunneling is established.

3. All VPN Authorized Users assume responsibility to assure that unauthorized users do not access City Technology Resources through their devices, software or configurations. This includes Authorized User's family members, friends, and associates.

4. Device security controls must be maintained to City standards in all unsecured remote locations. Exceptions require bureau director, CTO and SISO

5. Because 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 MFA.

6. For non-City Authorized Users such as vendors and contractors, the responsible Business System Owners must identify remote technology resource access requirements with proper written justification of the business reasons for such access. Additionally, remote access for vendors or contractors must only be enabled during the time needed, disabled when not in use, and promptly deactivated after access is no longer necessary. The SISO holds the final approval authority for all remote access to the City's network.

The following additional policies apply to Authorized Users approved for remote Office 365 access to City Technology Resources.

1. Bureau and BTS authorization are required for remote access to Office 365. Certain Authorized Users may have additional limitations related to remote access. See HRAR 4.04 Teleworking and HRAR 4.08 Information Technologies.
2. Office 365 access requires MFA when accessing City resources from unmanaged devices.
3. Office 365 access does not grant access to City resources and information stored within the City’s physical environment (local file shares, databases, endpoint device disk drives, or local applications.
4. City information must not be saved or stored on devices that are not City-owned, managed, or have not been approved and governed by City contract. See HRAR 1.03 Public Records Information, Access and Retention, and HRAR 11.04 Protection of Restricted and Confidential Information.
5. City information and records must be managed in accordance with State and City Rules Related to Public Recordkeeping Requirements. (https://www.portlandoregon.gov/archives/70031)

Exceptions to this policy, or any sections thereof, may be granted on a case-by-case basis by the CTO and the SISO. If an exception is granted for VPN technology on non-City devices, Authorized Users acknowledge that their devices are a de facto extension of the City's networks and as such, are subject to all policies that apply to City

Authorized Users and City-owned and managed assets, including, but not limited to acceptable minimal security standards of operating systems and software.

Responsibility

BTS 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, approved operating systems, operating systems patches, active firewalls, as well as other security and remote administration tools.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

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

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.
Reviewed and revised by Chief Information Security Officer of Bureau of Technology Services on October 23, 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.