BTS-2.03 - Network Access

NETWORK ACCESS
Administrative Rule Adopted by Council
ARC-BTS-2.03

Purpose
Access to resources on the City network is essential for many City employees to do their job. At the same time, security considerations require that access is limited to only those persons whose responsibilities require access, and to only those resources required to fulfill their duties.

The purpose of the Network Access Policy is to establish rules for the access and use of the City's network infrastructure.

Administrative Rule
Access to the City's network and applications will be made available to all Bureaus, Offices and locations and follow a standard process to determine access requirements for:

- City personnel
- Citizens and business partners
- Contracted support personnel

City employees will be given access to only those specific resources actually required to accomplish their job as determined by Business Systems Owners and Data Custodians.

Non-City employees will not be given access to the City's network, except on a case-by-case basis or by Council action (e.g. Intergovernmental Agreements). Any non-City employee receiving permission to access the City's network must abide by all City Information Technology policies, standards and procedures.

Security-warning banners must be displayed prior to allowing the logon process to be initiated by users. This security banner must inform all users that the network being accessed is proprietary, should only be accessed by authorized users, and that system use is monitored for enforcement purposes.

Responsibility

Bureau Responsibilities

- Business System Owners and Data Custodians shall identify those employees who require access to the City network, including specific network resources and applications. These approved authorizations shall be in writing and maintained by BTS.
- Business System Owners and Data Custodians shall identify the minimum required account access required for an employee to effectively fulfill their responsibilities.
- For non-City employees, the responsible Bureau Manager must identify 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. Requests for such access can be made by completing the appropriate request form. http://www.portlandonline.com/omf/index.cfm?c=39147
- Business System Owners and Data Custodians or a designated Bureau of Human Resources representative, are responsible for immediately notifying the BTS Helpdesk when access to City information systems should be discontinued. Specific examples included termination of employment or assignment to responsibilities and duties for which access is no longer required.
- Data Custodians, or those who manage Bureau specific data which can be accessed by multiple users, are responsible to conduct bi-annual audits to ensure assigned users continue to require access. Any required changes of access rights should be immediately reported to the Bureau of Technology Services.

Bureau of Technology Services Responsibilities

- Create and delete user accounts, grant and revoke access to appropriate computing resources as defined by the Business System Owners and Data Custodians following established policies and procedures.
- Disable all user accounts found to be inactive for a period of 90 days.
- Delete all user accounts that have been disabled for a period greater than 1 year.
- Respond to bureaus for specific help needed to audit network access.

History
Originally published as PPD number ARC-BIT-2.04, 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-2.03.