BTS-2.14 - Security Audits

SECURITY AUDITS
Administrative Rule Adopted by Council
ARC-BTS-2.14

Purpose
This policy outlines the authority for employees of the City's Information Security Office, in cooperation with BTS Operations, to conduct security audits on information systems at the City.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents and to ensure compliance to City security policies
- Monitor user or system activity where appropriate.

This policy covers all computing and communication devices owned or operated by the City. This policy also covers any computing and communications devices that are present on City owned premises or connect to the City network, but which may not be owned or operated by the City.

Administrative Rule
When requested, and for the purpose of performing an audit, necessary access will be provided to members of the City's Information Security Office and appropriate BTS Operations personnel. This policy does not supersede the requirement that the City auditor or other appropriate Bureau Directors approve access to the information, such as when it is restricted by law or State/Federal requirement.

This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on City equipment or premises.
- Access to work areas (data centers, computer rooms, telephone closets, labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on City networks.

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