BTS-2.14 - Security Audits

SECURITY AUDITS

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.14

Purpose

This policy outlines the authority for employees of the City's Information Security Office to conduct security audits of technology 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 with City security policies
- Monitor user or system activity where appropriate.

This policy covers all technology devices owned or operated by the City. This policy also covers any technology devices that are present on City owned premises or connected 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. This policy does not supersede the requirement that the City auditor or other appropriate Bureau Directors approve access to the technology system, 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 technology device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on City technology 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.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.