BTS-2.13 - Intrusion Detection

INTRUSION DETECTION
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.13

Purpose
Intrusion detection plays an important role in implementing and enforcing the City's information security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Intrusion detection provides two important functions in protecting information resources:
- Feedback: Information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

The City Intrusion Detection Policy applies to all individuals that are responsible for the installation of new information systems, the operations of existing information systems, and individuals charged with information system security.

Administrative Rule

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be enabled.
- Audit logs from the perimeter access control systems must be monitored and reviewed by the system operators.
- System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
- Audit logs for servers and hosts on the internal, protected, network must be reviewed by the system operators.
- System operators will furnish any audit logs to the Information Security Office upon request.
- Audit log review, in conjunction with event correlation software, may be delegated.
- Host based and network based intrusion tools must be checked on a routine basis when and where implemented.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the BTS Rule 2.08 INCIDENT REPORTING & RESPONSE.

History
Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
This rule was reviewed as part of a periodic review and remains unchanged, 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 and remains unchanged. April 30, 2018.