BTS-2.13 - Intrusion Detection

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Policy category: Information Security

Policy number: BTS-2.13

INTRUSION DETECTION

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

ARB-BTS-2.13

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.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

BTS-2.13 Intrusion Detection Administrative Rule 106.5 KB

Search Code, Charter, Policy

Keywords

Search

BTS-2.13 - Intrusion Prevention and Detection

INTRUSION PREVENTION AND DETECTION

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

Purpose

Intrusion prevention and detection plays an important role in implementing and enforcing the City's Information Security Policy. As information technology services and systems grow in complexity, effective security protection systems must mature. With the proliferation of cybersecurity vulnerabilities introduced by use of internetworking technologies a level of assurance is needed that City Technology Resources are secure. Intrusion prevention and detection systems provide an essential part of that assurance.

Intrusion prevention and detection provides two important functions in protecting City Technology Resources:

1. Feedback: Information as to the effectiveness of other components of information technology security systems and services. If a robust and effective intrusion prevention and detection system is in place, the lack of detected intrusions is an indication that other information security controls and defense capabilities are working.
2. Trigger: a mechanism that determines when to activate planned responses to an intrusion or policy violation incident.

The City Intrusion Prevention and Detection policy applies to all Authorized Users and all access to City Technology Resources. Additional responsibilities are assigned to technology support and administrative roles that are responsible for the installation of new information technology systems and services, the operations of existing information technology systems and services, and Authorized Users charged with information security.

Administrative Rule

1. Operating system, user accounting, and application software audit logging processes must be enabled on all endpoint (host), Internet-based Service Provider (Cloud) and server systems.
2. Alarm and alert functions of all firewalls and other network access control systems must be enabled.
3. Audit logging of all firewalls and other network access control systems must be enabled.
4. Audit logs from the access control systems must be monitored and reviewed by the service or system operators.

5. Service and system integrity checks of the firewalls and other network access control systems must be performed on a routine basis, as approved by the Information Security Office.
6. Audit logs for services, servers and hosts on the internal, protected, network must be reviewed by the responsible BTS Support Professionals, Business Systems Owners, or System Operators and System Administrators.
7. Audit logs for Internet-based Services Provider services must be reviewed by accountable City Authorized Users as defined within the terms of the service contract, applicable regulations, City and BTS policies and Administrative Rules.
8. System Operators and System Administrators will furnish audit logs to the Information Security Office upon request.
9. Audit log review, in conjunction with event correlation software, may be delegated to authorized service and system technical custodians.
10. Endpoint-based (host) and network-based intrusion prevention and detection tools must be audited on a routine basis as required by applicable regulations, City and BTS rules, policies and Administrative Rules.
11. All critical and high threat alerts and reports of anomalous activity must be reported to and reviewed by BTS Support Professionals for symptoms that might indicate unauthorized access or cyber threat activity. The Information Security team will assess whether an Incident Response plan activation is warranted.
12. All suspected or confirmed instances of unauthorized access, misuse or abuse of City Technology Resources must be immediately reported by Authorized Users and BTS staff according to the BTS Rule 2.08 INCIDENT REPORTING & RESPONSE.

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

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.

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.