BTS-2.12 - Physical Security

PHYSICAL SECURITY
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.12

Purpose
This policy describes the methods and responsibilities for protecting physical computer, network, communications and information resources. The City requires that appropriate environmental, protection and access controls be in place to protect computing and information resources. Proper and adequate physical security and protection is the responsibility of all City employees.

Physical Security
Physical security measures are an important part of any effort to protect technology assets and services. As with logical security measures at the City, physical security measures required for protecting City computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. Control measures will be applied in accordance with systems environment sensitivity and criticality.

The City has a wide spectrum of information systems deployments. They include:

- Desktop computer workstations and printers operated in an office environment.
- Wireless and mobile devices such as laptops, radios, mobile phones and any other personal computing device which are operated both in an office environment and at remote locations.
- Small sets of individual Bureau servers located in office environments.
- Computer labs which host computing and network equipment used for testing and development purposes.
- Telecommunications closets which contain network and communications equipment and wiring.
- Media storage areas or vaults which are used to store electronic media such as backup tapes, surplus equipment and classified documents.
- Modest-sized server rooms which host a limited number of computing devices and networking equipment.
- Enterprise data center facilities that host a wide variety and large quantity of critical computing equipment such as mainframes, servers, tape libraries, storage arrays and network equipment.

All of these technology deployments require varying levels of physical security commensurate with the criticality of the systems and information involved. Regardless of the specific environment, the City requires physical security requirements to be supported by all Business System Owners, Data Custodians, System Operators, and Users.

Administrative Rule
At a minimum, the following physical security measures and objectives must be implemented where applicable to protect City technology assets, and sensitive information:

- Mainframes, servers, network equipment, computer media containing sensitive data and other essential computer and network devices shall be stored in a secure location, such as a locked room, that protects them from unauthorized physical access, use, misuse, destruction or theft.
- Smoke/fire alarm and suppression systems are required for all data centers, server rooms and telecommunication closets to mitigate personnel harm and/or damage to City assets in the event of a fire.
- Temperature and ventilation control measures are required for all data centers and server rooms to protect City assets from preventable service disruptions or physical harm from environmental conditions.
- All mission critical data centers must employ emergency power control systems (backup generators and uninterruptible power supplies) to avoid disruptions and/or equipment/data harm due to power related failures.
- Inventory control measures such as inventory reports, asset tags or other identification markings for tracking are required per City accounting policy.

- All access to restricted areas, such as data centers, server rooms, and telecommunications closets, by unauthorized individuals must be conducted with an authorized City employee escort at all times.
- Access keys and key codes to restricted areas must be limited to only those individuals needing entry to fulfill their job responsibilities. Records of individuals' assigned access must be maintained.
- All specific tools, systems, or procedures implemented to meet physical security requirements must be selected on the basis of importance to safety, security and compliance with City policies and standards.

All City employees must be responsible to secure information assets in their care and possession and immediately report any loss or theft of such assets to their management and the Bureau of Technology Services. Additionally, all City employees must be aware of unauthorized individuals (e.g. maintenance, public and others visiting, delivery personnel, vendors, etc.) and be prepared to challenge individuals entering data centers, computer rooms and other restricted areas.

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.
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.