BTS-2.12 - Physical Security

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

Policy category: Information Security

Policy number: BTS-2.12

PHYSICAL SECURITY

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

ARB-BTS-2.12

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.

Revised by Chief Technology Officer October 10, 2018.

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

Related documents

BTS-2.12 Physical Security Administrative Rule 107.22 KB

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 Citywide physical computer, network, communications and City Technology Resources. The City requires that appropriate environmental controls, physical 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 Authorized Users.

Physical Security
Physical security measures are an important part of any effort to protect City Technology Resources and City technology services. As with administrative security measures at the City, such as policies and standards, physical security measures required for protecting City Technology Resources must be commensurate with the nature and degree of criticality of the computer systems, network resources, connectivity and information classification involved. Physical security control measures will be applied in accordance with physical and environmental considerations, compliance regulations, information privacy and confidentiality, and service criticality.

The City provides a wide spectrum of City Technology Resources. They include, but are not limited to:

1. Desktop computer workstations and printers operated in office and facility environments, as well as home office and telework locations.
2. Wireless and mobile devices such as laptops, radios, smartphones and any other personal computing device which are operated both in an office environment and at remote locations.
3. Small sets of individual Bureau servers located in office and remote location environments.
4. Computer labs which host computing and network equipment used for testing and development purposes.
5. Telecommunications closets which contain network and communications equipment and wiring.
6. Media storage areas and vaults which are used to store electronic media such as backup disk drives, surplus equipment, as well as classified and archival documents.
7. Modest-sized server rooms which host a limited number of computing devices and networking equipment.
8. Enterprise data center facilities that host a wide variety and large quantity of critical computing equipment such as technology appliances, servers, data libraries, information storage arrays and network equipment.

9. Internet-based Service Provider services that provide software as a service (SaaS) and information technology services that extend the City's networking environment.

Technology deployments require varying levels of physical security commensurate with the service criticality of the systems and the confidentiality of the 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 Authorized Users.

Administrative Rule

At a minimum, the following physical security measures and objectives must be implemented where applicable to protect City Technology Resources, and City Confidential and Restricted Information:

1. Technology appliances, servers, network equipment, computer media containing City Confidential and Restricted Information and other essential computer and network devices must be stored in a secure location, such as a locked room, that protects them from unauthorized physical access, use, misuse, destruction or theft.
2. 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 Technology Resources in the event of a fire.
3. Temperature and ventilation control measures are required for all data centers and server rooms to protect City Technology Resources from preventable service disruptions or physical harm from negative environmental conditions.
4. 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.
5. Inventory control measures such as inventory reports, asset tags or other identification markings for tracking are required per City accounting policy.
6. All access to restricted areas, such as data centers, server rooms, and telecommunications closets, by unauthorized individuals must always be conducted with an authorized City employee escort.
7. 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. Access logs must be maintained for at least one year, at a minimum, or if applicable regulations require. Access approval shall be 'minimum necessary' and 'need to know' in keeping with regulatory and applicable City Administrative Rules.
8. All specific tools, systems, or procedures implemented to meet physical security requirements must be selected based on importance to safety, information and physical security and compliance with City Administrative Rules, policies and standards.

All Authorized Users must be responsible to secure City Technology Resources in their care and possession and immediately report any loss or theft of such assets to their management and the BTS HelpDesk. Additionally, all Authorized Users must be aware

of Unauthorized Users (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. Attempts by Unauthorized Users to access City Technology Resources or facilities must be reported to the OMF Facilities Security office.

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.
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.
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.