BTS-2.15 - Encryption

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

Policy category: Information Security

Policy number: BTS-2.15

ENCRYPTION

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

ARB-BTS-2.15

Search Code, Charter, Policy

Keywords

Search

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.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD 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. 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-2.15 Encryption Administrative Rule 105.39 KB

BTS-2.15 - Encryption

ENCRYPTION
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.15

Purpose
Encryption standards and technologies are used to prevent Unauthorized Users from accessing or altering Confidential or Restricted Information stored on City Trusted Networks and City Technology Resources, Hosted Technology Resources, or transmitted across City and public networks.

The purpose of this policy is to provide guidance for where encryption technologies must be implemented and limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that State and Federal regulations are observed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Administrative Rule

Applicability
Approved encryption standards and techniques for the storage and transmission of City Confidential and Restricted Information must be implemented based on a) information classification, as defined in BTS Administrative Rule 2.18 Information Classification & Protection (https://www.portlandoregon.gov/citycode/article/394545) and, b) information security risk management decisions established by the Chief Technology Officer (CTO), Senior Information Security Officer (SISO) and Business System Owner, unless expressly required and defined by regulation, statute or contractual obligation.

The following classifications of Confidential and Restricted Information are expressly subject to the City's Encryption Policy:

1. Criminal justice information (CJI) when transmitted across public networks or any private network that is shared with non-criminal justice Authorized Users
2. Authorized User or application level credentials (account names & passwords)
3. Payment Cardholder Data (PCI) including primary account number, cardholder name, expiration date, and service or security code or Personal Identification Number (PIN)
4. Personally identifiable information (PII) as defined by the Oregon Consumer Information Protection Act
5. Electronic protected health information (PHI) such as health benefit information covered under HIPAA privacy regulations
6. Any 802.11 wireless or Remote Network Access communications when used to connect to the City's Trusted Networks or City Technology Resources

7. Confidential and Restricted Information stored on Mobile Computing Devices, such as laptops, smartphones, and Removable Media, such as USB thumb drives

Note: This is not a complete list and is provided to give general guidance for commonly used Confidential and Restricted Information subject to higher levels of information security protection. Please contact the BTS Information Security Office for appropriate classification of data and to help determine if encryption is required. See also BTS 2.18 Information Classification & Protection (https://www.portlandoregon.gov/citycode/article/394545)

Additional Considerations

Where networks and systems are under legal regulations such as Criminal Justice Information Systems (CJIS) Policy, there may be additional encryption requirements above and beyond the City's encryption policy.

Criminal Justice Information is restricted to authorized United States agency use within U.S. borders.

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.
Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD 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. 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.