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 technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive data stored on City systems and network 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 techniques for the storage and transmission of City information shall be implemented based on security risk management decisions which will be at the discretion of the Chief Technology Officer (CTO) or Chief Information Security Officer (CISO) and Business System Owner unless expressly required by legal regulation, statute or contractual obligation.

The following types of sensitive or confidential information shall be subject to the City's Encryption Policy:

- Criminal justice data when transmitted across public networks or any private network that is shared with non-criminal justice users
- User or application level credentials (account names & passwords)
- Payment Cardholder Data including primary account number, cardholder name, expiration date, and service code
- Personally identifiable information as defined by the Oregon Identity Theft Protection Act.
- Electronic protected health information (ePHI) such as health benefit data covered under HIPAA privacy regulations
- Any 802.11 wireless or Remote Network Access communications when used to connect to the City's networks or computing resources
- Confidential data stored on portable computing devices such as laptops, smartphones, and USB thumb drives

Note: This is not a complete list and is provided to give general guidance on commonly used confidential/sensitive information subject to higher levels of protection. Please contact BTS Information Security for appropriate classification of data and to help determine if encryption is required.

Encryption Standards
Proven, standard algorithms shall be used as the basis for encryption technologies. Symmetric cryptosystem key lengths must be at least 128 bits. BTS will periodically review City encryption key length requirements and upgrade them as technology allows.

- Use the following encryption protocols; TLS 1.1, 1.2, or higher. SSLv2 and SSLv3 are deprecated protocols and are prohibited. TLS 1.0 shall only be used if higher versions of TLS are not available.
- Use the following digital signature algorithms; RSA, DHE (2048+ bits), ECDHE.
- Use the following encryption algorithms; AES-128, AES-256 or 3DES-168. RC4 is deprecated and is prohibited.
- Use the following hashing algorithm; SHA1 or better. MD5 is deprecated and is prohibited.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the CTO or the CISO.

Export Restrictions
The export of encryption technologies is restricted by the U.S. Government.

Criminal justice information is restricted to authorized United States agency use within U.S. borders.

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.

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.