BTS-2.15 - Encryption

ENCRYPTION
Administrative Rule Adopted by Council
ARC-BTS-2.15

Purpose
Encryption technologies are used to prevent unauthorized individuals from reading or altering confidential or sensitive data stored on City systems or transmitted across City and public networks.

The purpose of this policy is to provide guidance as for where encryption technologies are to 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 information shall be implemented based on security risk management decisions which will be at the discretion of the CTO or delegate in consultation with the Information Security Manager and Business System Owner unless expressly required by legal regulation, statute or contractual obligation.

In general, the following types of sensitive or confidential data may 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)
- Credit card account numbers
- Data, when used together, results in a high risk for identity theft such as name, address, social security number & date of birth
- 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 internal networks
- Confidential data stored on portable/mobile computing devices such as Laptops, PDA's and USB Thumb Drives which have a greater likelihood of loss or theft

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

Encryption Standards
Proven, standard algorithms such as 3DES, AES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

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 delegate, in consultation with the Information Security Manager (ISM).

City encryption key length requirements will be reviewed periodically and upgraded as technology allows.

Export Restrictions
Be aware that the export of encryption technologies is restricted by the U.S. Government.

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.