Encryption Policy

The Policy

All City of New York data with a data classification of private or confidential may not be stored and/or transmitted across any communication mechanism unless it is protected using approved data encryption technology.

Background

Encryption is a method of protection that ensures the confidentiality of data. Use of encryption technology significantly limits unauthorized access to business critical information. To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope

This policy applies to all information classified as private or confidential that may be transmitted by electronic means. Electronic information is defined as data, stored electronically, copied, and/or transmitted concerning the City of New York business, information systems, employees, business partners, or customers.

Approved Use

1) Only City of New York approved cryptographic algorithms and supporting processes as defined in the Citywide Encryption Standard may be used to protect business critical information and ensure interoperability with other agencies.

Data At Rest

2) Private or confidential data stored in a database or file system (at rest) must be encrypted in accordance with the Citywide Encryption Standard. Alternatively, approved database security gateway technology may be used in lieu of encryption to protect private data at rest.
3) The use of password protection instead of encryption is not an acceptable alternative to protecting private information.

Removable Media

4) Data categorized as private or confidential should not be transitioned to removable media without management approval.
5) Removable media including CDs, backup tapes, and USB memory drives that contain private or confidential data must be encrypted and stored in a secure location.
6) When transferring removable media the receiver must be identified to ensure the person requesting the data is a valid recipient.

Transmission Security

7) Private or confidential data sent across any network connection must be encrypted in

accordance with the Citywide Encryption Standard.

8) Unencrypted transmission of private or confidential data through web applications or email is not allowed.

9) Wireless networks must be encrypted using an approved City of New York standard.

Portable Devices

10) Private or confidential data may only be stored on portable devices such as laptops, smart phones and personal digital assistants (PDAs) when encrypted.

11) Portable devices should not be used for long-term storage of private or confidential data.

12) Where it is technologically feasible portable devices must have the capability to be remotely wiped in the event of theft or accidental loss.

13) Portable devices must have proper protections in place as outlined in the Citywide Portable Computing Information Security Policy.

Encryption Strength

14) Approved encryption algorithms must be of a minimum key length of 128 bits.

Key Management

15) Private keys must be kept confidential.

16) Key lifecycle management must be implemented.

17) Keys in storage and transit must be encrypted.

18) Keys must be chosen randomly from the entire key space.

19) Encryption keys must allow for retrieval for administrative or forensic use.

Document Revision History

Date	Description
April 3, 2008	**Version 1.0** Issued.
June 16, 2011	**Version 1.1** Updated header with new NYC logo and added this revision history table to the document.
October 12, 2011	**Version 1.2** Added the following text to bullet #2: "Alternatively, approved database security gateway technology may be used in lieu of encryption to protect private and/or confidential data at rest."
Aug 17, 2012	**Version 1.3** Updated bullet #7 (changed "across a network connection" to "any network connection." Updated bullet #8 (added "email"). Deleted bullet # 10 (Any private or confidential information transmitted to and from vendors doing business with the City of New York must be encrypted or transmitted in a secure fashion." (redundant)