Data Classification Policy

The Policy

The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background

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. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

Information Classification

All information at the City of New York and corresponding agencies will be classified at one of four levels; public, sensitive, private, or confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency's ability to perform its primary business function. Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as confidential.

Information Valuation and Categorization

1) 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.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Data Steward

5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.

7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.

8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Information Labeling

9) Information within systems or processes must be marked appropriately to ensure that users will be aware of the sensitivity of the information and how it should be protected and controlled. Appropriate marking of mission critical information includes marking it as public, sensitive, private, or confidential.

10) All copies or reproductions maintain the same level of classification as the original.

11) Aggregation of data with different classification levels require reevaluation to determine if a new level of classification is needed.

12) All personally identifiable information should be classified at a minimum as private.

Information Protection

13) Protective measures must take into account the value associated with unauthorized access or loss of information assets.

14) Private or confidential data sent across any network connection must be encrypted in accordance with the Citywide Encryption Standard.

15) Private or confidential data stored in a database or file system 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.

Document Revision History

Date	Description
July 28, 2008	**Version 1.2** Issued.
June 16, 2011	**Version 1.3** Updated header with new NYC logo and added this revision history table to the document.
Aug 17, 2012	• **Version 1.4** Update description of confidential data on page 1 (added “Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as CONFIDENTAL.” • Added bullets 14 and 15 to match the language used in Encryption Policy.
Sept. 9, 2014	**Version 1.5** Policy review and minor formatting updates.