Information Security Policy for Service Providers

Scope

This policy applies to all vendors, subcontractors and other third parties which provide information technology services (generically, “Service Providers”) to the City of New York (“City”) and its agencies (“Agencies”).

Policy

Agencies must ensure that Service Provider agreements include the following language:

1) Service Provider agrees to comply with all Citywide Information Security Policies and Standards as published by DoITT, and which are annexed to and hereby made a part of this Agreement as Exhibit [___].

2) Service Provider shall provide written acknowledgement of receipt of the Citywide User Responsibilities Policy and appropriate Agency non-disclosure agreements and distribution of same to its employees and consultants.

3) Service Provider shall also ensure that any products, services and other deliverables which it provides to Agency are compliant with all Citywide Information Security Policies and Standards. Deliverables must be able to pass the Citywide Security Accreditation Process where applicable.

4) Service Provider shall use industry standards to ensure that it does not introduce any viruses or any other form of malicious code to City systems.

5) Service Provider shall cooperate with and facilitate the successful completion of any Security Accreditation tasks and processes relevant to the services and/or deliverables it provides.

6) Service Provider shall conduct background checks for each consultant assigned to the project in order to reduce the risk of human error, theft, or misuse of the City’s information assets. When requested, Service Provider will provide documented evidence of background checks for each consultant assigned to the project.

7) The City of New York reserves the right to audit the IT infrastructure and information security controls and processes of the Service Provider and to perform relevant tests to ensure that it is compliant with Citywide Information Security Policies and Standards. Service Provider will permit the City to perform an IT audit, including an audit of physical security of any Service Provider premises applicable to the engagement and will cooperate and furnish all requested materials in a timely manner.

8) When requested, Service Provider agrees to provide evidence of an independent IT security review or audit commensurate with the security requirements of the project. This audit must be completed within a time frame specified by the City.

9) Service Provider shall surface issues, suggest options, and make recommendations to the City with regard to information security, based on the classification of data as described in the City's Data Classification Policy. This includes all material issues identified, regardless of infrastructure ownership.

10) Service Provider shall identify and provide contact information for the person who has been assigned overall responsibility for information security within its organization. When requested, Service Provider agrees to provide a copy of its information security policies.

11) A Service Provider may not export City data classified as “CONFIDENTIAL outside the United

States except with the express written permission of the Agency head. "CONFIDENTIAL" shall have the meaning ascribed to in the City's Data Classification Policy, which is annexed to and hereby made a part of this Agreement as Exhibit [___].

12) Service Provider must obtain written permission from Agency for each method of remote access it wishes to use to access City data.

13) Should Service Provider learn or suspect that there has been a breach of this policy, it shall immediately notify its Agency liaison and the Citywide Service Desk.

14) Violations of any part of this policy or any other Citywide Information Security policies, standards, procedures or other security requirements shall constitute a material breach of the Agreement.

15) Agencies may impose additional and more stringent information security requirements than those in this policy.

16) The Service Provider's obligations under this policy shall survive the termination or expiration of the Agreement.

Document Revision History

Date	Description
March 16, 2012	**Version 1.0** Initial publication
Sept. 9, 2014	**Version 1.1** Policy review and minor formatting updates.