Attachment V - SCY
(Security Requirements)

Systems Integration Services for Technology Projects Citywide

for

ONE NUMBER CALL CENTER SOLUTION REQUEST FOR SERVICES (RFS)
PIN: 21GPMMI13201

1. Definitions

(a) *"City"* means The City of New York and/or a county, borough, or other office, position, administration, department, division, bureau, board or commission, or a corporation, institution or agency of government, the expenses of which are paid in whole or in part from The City of New York's treasury.

(b) *"City Information Assets"* means all City computer systems, electronic data stored, processed, transmitted, or printed by City computer systems, and such systems' peripheral equipment, networks, or magnetic data, as well as any cloud computing system maintained by the City or any non-City entity for the City's use, and any electronic data stored, processed, transmitted, or printed by such system.

(c) *"Contractor"* means a person or entity engaged by the City of New York to perform tasks pursuant to the Agreement.

(d) *"Facility(ies)"* means a physical structure operated by the City of New York.

(e) *"Person"* means an officer, agent or employee of the Contractor or a subcontractor of the Contractor.

(f) *"Project"* means any type of work to be performed pursuant to the Agreement.

(g) *"Security Investigation"* means a criminal history and background investigation in accordance with the requirements set forth herein. The City reserves the right to modify the scope of requisite investigations upon provision of reasonable notice to the Contractor.

2. Citywide Information Security Policy

All Persons, who may have access to any City Confidential Information or City Information Assets, in the course of carrying out their responsibilities or job function must comply with the Citywide Information Security Policies and Standards ("Policies and Standards") established by DoITT as it may be modified from time to time, which are available on CityShare at http://cityshare.nycnet/infosec and at

https://www1.nyc.gov/site/doitt/business/it-security-requirements-vendors-contractors.page and will also be provided upon request.

3. DoITT User Responsibility Policy

The Contractor shall require that all Persons in the Contractor's or subcontractors' organizations who may have access to any City Information Assets in the course of performing work pursuant to the Agreement will be provided a copy of DoITT's "User Responsibility Policy" ("URP"); *which is not required at this time*, and the Contractor shall be required to sign the

acknowledgement of same, prior to performing work. The Contractor shall provide a signed copy of the URP for each such Person to the DSS Project Manager or a person designated by DoITT within fifteen days (15) days after a Person is assigned to a Project.

4. Security Investigation

The City may, prior to or during the course of a Project, request that the Contractor require a Person, or Persons, associated with a Project to undergo a Security Investigation before being granted access, or continued access, to Facilities, City Confidential Information or City Information Assets.

If Security Investigations are requested or required by the City prior to the commencement of a Project, the Contractor is required to submit the results of the Security Investigation for each Person that it proposes to assign to perform services on the Project sufficiently in advance to ensure that all security clearance procedures are complete without delaying the Contractor's work performance. The City shall not be liable for payments or damages of any kind if the Contractor's work is delayed or the Contractor is required to assign different individuals on account of the City's reasonable delay or refusal to grant an individual a security clearance under the Agreement.

The Contractor shall assume, without any reimbursement by the City, all costs incurred in connection with the investigations.

Where an emergency or other circumstance occurs which renders immediate compliance impractical, the City may, in its sole judgment, defer a Person's compliance and grant temporary access, pending the results of the Security Investigation. Such deferment shall not be construed as a waiver of the City's right subsequently to require that a Security Investigation be performed.

The City reserves the right, in its sole discretion, to refuse access to City Facilities, City Confidential Information or City Information Assets: (i) to any individual who refuses to comply with the security or non-disclosure procedures required by the City or (ii) where the City determines that the individual may present a risk to its security interests.

5. Compliance with Other Security Policies and Procedures

The Contractor shall require that all Persons working on the Project comply with all applicable Facility, data processing and other security policies and procedures of the City in effect for the duration of the Project, including but not limited to Internet usage, office equipment usage and timekeeping procedures. This may include being required to sign in and out and enter time worked into a timekeeping system provided by the City.

6. Notification of Termination, Reassignment or Cessation of Access

The Contractor shall promptly notify the City liaison assigned to the Project, in writing, when any Person previously engaged by the Contractor to gain access to any Facilities, City Confidential Information or City Information Assets is no longer authorized by the Contractor to do so, and the Contractor shall make reasonable efforts to prevent any such Person from accessing any Facilities, City Confidential Information or City Information Assets from the point in time that such individual's authorization ceases.

7. Non-Disclosure Agreement

If reasonably requested by the City, the Contractor shall require its officers, agents, employees and subcontractors who either work in direct support of the Project or who may reasonably be anticipated to unintentionally receive City Confidential Information to execute a Non-Disclosure Agreement in an appropriate form.

8. Contractor-Provided Equipment

The Contractor shall ensure that any products, services and other deliverables it provides to the City Agency are compliant with the Policies and Standards.

9. No Introduction of Viruses

The Contractor shall use industry standards to ensure that it does not introduce any viruses or any other form of malicious code to City systems.

10. Cooperation with Accreditation

The Contractor shall cooperate with and facilitate the successful completion of any security accreditation tasks and processes relevant to the services and/or deliverables it provides.

11. Contractor's Policies

Upon request, the Contractor shall, pursuant to a clean room disclosure process, provide a copy of its information security policies relevant to this Agreement.

12. City Audit(s)

The City reserves the right to audit the IT infrastructure and information security controls and processes of the Contractor and to perform relevant tests to ensure that it is compliant with the Policies and Standards. The Contractor will permit the City to perform an IT audit, including an audit of physical security of any of the Contractor's premises applicable to the

services provided pursuant to this Agreement and will cooperate and furnish all requested materials in a timely manner. For the avoidance of doubt, so long as the Services are not provided on Contractor IT infrastructure, then Contractor does not have to submit its IT infrastructure to the requirements of this paragraph.

13. Independent Review(s)/Audit(s)

Upon request, the Contractor shall provide evidence of an independent IT security review or audit commensurate with the security requirements of the Project. within a time specified by the City. The scope of the review/audit and the time by which the Contractor must provide evidence of the review/audit shall be determined in the City's sole discretion. For the avoidance of doubt, so long as the Services are not provided on Contractor IT infrastructure, then Contractor does not have to submit its IT infrastructure to the requirements of this paragraph.

14. Suggestions

The Contractor may surface issues, suggest options, and make recommendations to the City with regard to the Policies and Standards where appropriate.

15. Liaison

At the beginning of the Term of this Agreement, the Contractor shall identify and provide contact information for the Person who has been assigned overall responsibility for information security within its organization.

16. No Exporting of City Data Outside United States

The Contractor may not export City Confidential Information outside the United States except with the express written permission of the Commissioner of DSS (Department of Social Services) and then only for the City Confidential Information specified in that permission.

17. Remote Access Methods

The Contractor must obtain written permission from DoITT for each method of remote access it wishes to use to access City Information Assets.

18. What to Do in Case of a Breach

Should the Contractor learn or suspect that there has been a breach of its obligations under this Attachment, it shall immediately notify its DoITT liaison and the DoITT Service Desk. The Contractor shall then cooperate fully in any government investigation into any such possible breach.

19. Material Breach

Violations of any part of this Attachment or any of the Policies and Standards shall constitute a material breach of this Agreement.

20. Headings

Headings are inserted only as a matter of convenience and for reference and in no way define, limit, augment or describe the scope or intent of this Attachment.