ATTACHMENT SCY
Security Requirements

1. DEFINITIONS

(a) "**Agreement**" means the Agreement between the Contractor and DOHMH, annexed hereto.

(b) "**Authorized Person**" has the meaning given below in Section 16(a).

(c) "**Authorized Subcontractor**" has the meaning given below in Section 16(a).

(d) "**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, including Cyber Command, the expenses of which are paid in whole or in part from the City of New York's treasury, or an entity created under New York law specifically for the benefit of the City or to serve persons present in the City of New York and that has 1 or more members or directors of which are appointed by the mayor or City Council (e.g., the New York City Board of Elections).

(e) "**DOHMH**" means the New York City Department of Health and Mental Hygiene.

(f) "**DOHMH Data**" means (1) Data characterizing DOHMH or its behavior; (2) Data owned, created, generated, stored or maintained by, at the direction of, or for the benefit of DOHMH; and (3) any copies or derivatives of such Data.

(g) "**Data**" means any information representation(s) of information, knowledge, facts, ideas, concepts or similar including any texts, instructions, documents, databases, diagrams, graphics, drawings, images, sounds, or biometrics that are accessed, communicated, created, generated, stored (in temporary or permanent form), filed, produced or reproduced, processed, referenced, or transmitted, in any form or media.

(h) "**DOHMH Technology Assets**" means all DOHMH Facilities, DOHMH Systems, DOHMH telecommunications, electronic data created, processed, accessed, transferred, stored, or disposed of by DOHMH Systems, and such systems' peripheral equipment, networks, or magnetic data, and any electronic data created, processed, accessed, transferred, stored, or disposed of by such systems, or data owned by DOHMH.

(i) "**DOHMH Systems**" means any system owned, maintained or operated by or on behalf of DOHMH that connects to a DOHMH network, enables operational functions of DOHMH, or creates, processes, accesses, transfers, stores, or disposes of DOHMH Data.

(j) "**Commissioner**" means the head of DOHMH.

(k) "**Contractor**" means a person or entity engaged by DOHMH to perform tasks pursuant to the Agreement.

(l) "**Cyber Command**" means the Office of Cyber Command, created by New York City Charter § 20-j, established within the New York City Office of Technology and Innovation ("**OTI**"), that is empowered to ensure compliance with Policies and Standards, lead citywide cyber defense, investigation and incident response, serve as the primary liaison between public (federal, state and tribal) and private partners/stakeholders for cyber intelligence sharing, investigation and response coordination, coordinate deployment of citywide technical and administrative controls related to information technology, information security and information privacy and review citywide cyber related procurements, in collaboration with procuring agencies.

(m) "**DoITT**" means the Department of Information Technology and Telecommunications, designated as the New York City Office of Technology and Innovation ("OTI") pursuant to Mayoral Executive Order No. 3 of 2022.

(n) "**Facility(ies)**" means a physical structure, such as a data center or other building.

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

(p) "**Policies and Standards**" means the Citywide Information Security Policies and Standards, Cyber Command Policies and Standards, or any policies and procedures by OTI, available at https://www1.nyc.gov/content/oti/pages/vendor-resources/cybersecurity-requirements-for-vendors-contractors, as they may be amended or placed on a successor site by the City.

(q) "**Process**" means to perform any act, omission or operation on or with respect to data, such as collecting, recording, organizing, storing, adapting, altering, retrieving, accessing, deleting, blocking, erasing, destroying, combining, reviewing, using, transmitting, disseminating or otherwise making data available.

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

(s) "**Contractor Systems**" means the Facilities, systems, networks and IT environments that are used to Process any DOHMH Data, deliver any Services or to otherwise meet any of Contractor's obligations under the Agreement.

(t) "**Security Incident**" means an event that compromises or is suspected to compromise the security, confidentiality, integrity, or availability ("SCIA") of DOHMH Data, DOHMH Technology Assets or Contractor Systems, including by compromising the physical, technical, administrative or organizational safeguards implemented by Contractor to protect the SCIA of DOHMH Data, DOHMH Technology Assets or Contractor Systems. Examples of a Security Incident include, but are not limited to, the unauthorized acquisition or use of unencrypted DOHMH Data (or encrypted DOHMH Data and the decryption key), intrusions, virus or malware, ransomware infections, social engineering, missing/stolen hardware, a breach of access credentials, DDOS and DoS attacks

(u) "**Security Investigation**" means a criminal history and background investigation in

accordance with the requirements set forth herein. DOHMH reserves the right to modify the scope of requisite investigations upon provision of reasonable notice to the Contractor.

(v) "**User Responsibility Policy**" or "**URP**" means the User Responsibilities Policy available at https://www1.nyc.gov/assets/oti/downloads/pdf/vendor-resources/user-responsibilities.pdf, as it may be amended or placed on a successor site by the City.

(w) "**Services"** means the professional services the contractor is providing DOHMH.

2. CITYWIDE INFORMATION SECURITY POLICY

The Contractor shall comply with the Policies and Standards, and terms of the Agreement. In addition, the Contractor shall ensure that all Authorized Subcontractors and Authorized Persons who may have access to any DOHMH Data or DOHMH Technology Assets in the course of carrying out their responsibilities or job functions comply with the Policies and Standards.

3. USER RESPONSIBILITY POLICY

The Contractor will be provided with online access to, or a copy of, the User Responsibility Policy. The Contractor shall require each Authorized Person (as defined below in Section 16(a)) who may have access to any DOHMH Technology Assets to sign a written acknowledgement and agreement to comply with its terms prior to his or her assignment to perform any Services. The Contractor shall provide a signed copy of the URP acknowledgement for each Authorized Person to DOHMH project manager, or a person designated by DOHMH, within fifteen days (15) days after the Authorized Person is assigned to perform Services.

4. SECURITY INVESTIGATION

(a) DOHMH may, prior to or during the course of the Agreement, request that the Contractor require a Person, or Persons, associated with the Services to undergo a Security Investigation before being granted access, or continued access, to Facilities, DOHMH Data, DOHMH Technology Assets or Contractor Systems. DOHMH may require the Contractor and associated Persons to undergo federal, state and local background checks, where authorized by applicable law, that conform to industry standards, including criminal history and/or background investigation. Persons assigned to the Project by or through the Contractor shall be required to submit Identifying Information to DOHMH, and may, to the extent authorized by applicable law, be required to submit fingerprints. The Contractor and associated Persons agree to be subject to a background screening and checks, which may include the following:

( ) Employment Verification;
(i) Education Verification;
(ii) Reference Verification;
(iii) Criminal Record Check;
(iv) Civil Court Records Check;

(v) Professional License Check;
(vi) Credit History Check;
(vii) International Background Check; and
(viii) Terrorist Watch List Check.

(b) If Security Investigations are requested or required by DOHMH prior to the commencement of work by the Person, the Contractor is required to submit the results of the Security Investigation for each Person that it proposes to assign to perform services sufficiently in advance to ensure that all security clearance procedures are complete without delaying the Contractor's work performance. DOHMH 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 DOHMH's reasonable delay or refusal to grant an individual a security clearance under the Agreement.

(c) The Contractor shall assume, without any reimbursement by DOHMH, all costs incurred in connection with the investigations.

(d) Where an emergency or other circumstance occurs which renders immediate compliance impractical, DOHMH 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 DOHMH's right subsequently to require that a Security Investigation be performed.

(e) DOHMH reserves the right, in its sole discretion, to refuse access to DOHMH Data or DOHMH Technology Assets: **(i)** to any individual who refuses to comply with the security or non- disclosure procedures required by Cyber Command or **(ii)** where the Cyber Command determines that the individual may present a risk to its security interests.

5. COMPLIANCE WITH OTHER SECURITY POLICIES AND PROCEDURES

In addition to the Policies and Standards and the User Responsibility Policy, the Contractor shall comply with, and ensure that all Authorized Subcontractors and Authorized Persons comply with, all applicable Facility, data processing and other security policies and procedures of the Cyber Command in effect for the duration of the Agreement, including, but not limited to, processing, handling and storage of Restricted and Sensitive Information, 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 DOHMH.

6. NOTIFICATION OF TERMINATION, REASSIGNMENT OR CESSATION OF ACCESS

The Contractor shall promptly notify Cyber Command and the DOHMH liaison assigned to the Services, in writing, when any Person previously engaged by the Contractor to gain access to any Facilities, DOHMH Data, DOHMH Technology Assets or Contractor Systems 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, DOHMH Data or DOHMH Technology Assets from the point in time that such individual's authorization ceases.

7. **NON-DISCLOSURE AGREEMENT.** If reasonably requested by DOHMH, the Contractor shall require its Authorized Subcontractors and Authorized Persons who either work in direct support of the Services or who may reasonably be anticipated to unintentionally receive DOHMH Data to execute a Non-Disclosure Agreement in a form acceptable to DOHMH.

8. CONTRACTOR-PROVIDED EQUIPMENT

The Contractor shall ensure that any products, services and other deliverables it provides to DOHMH 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 DOHMH 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. The Contractor shall complete said security accreditation tasks and processes within thirty (30) business days unless granted an extension by Cyber Command.

11. VENDOR SECURITY QUESTIONNAIRE

The Contractor shall complete and respond to all security questionnaires from DOHMH within thirty (30) business days.

12. CONTRACTOR'S POLICIES

Upon request, the Contractor shall provide a copy of its information security policies relevant to the Agreement.

13. 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 at any time. 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 the Agreement and will cooperate and furnish all requested materials in a timely manner. Cyber Command reserves the right to monitor the security posture of the Contractor throughout the course of the Agreement.

14. SOFTWARE SECURITY ASSURANCE (SSA) APPROVAL

The Contractor agrees to submit all devices, applications, systems, software and infrastructure used to support DOHMH Systems, pursuant to the Agreement, to security testing in compliance with the City's Software Security Assurance process. The Contractor understands and acknowledges that failure to meet the SSA process requirements can result in termination of the Agreement.

15. REQUIREMENTS FOR SYSTEMS PROVIDING CRITICAL FUNCTIONS

(a) If Contractor maintains systems that provide critical DOHMH capabilities and/or functions, Contractor shall provide DOHMH with reports verifying that all patches and configurations are up to date, as well as forecast all required changes for the next twelve (12) months.

(b) The Contractor shall ensure that all necessary capabilities and equipment potentially required to service critical technology in the event of an incident is locally available.

16. USE AND PROTECTION OF DOHMH DATA

(a) The Contractor shall hold DOHMH Data in the strictest confidence, and shall not disclose any DOHMH Data to any person or entity other than a subcontractor that has been approved by DOHMH in writing (each, an "**Authorized Subcontractor**") or an employee of the Contractor or an Authorized Subcontractor who needs to know DOHMH Data in order to perform the Contractor's obligations under the Agreement (each, an "**Authorized Person**").

(b) The Contractor shall ensure that each Authorized Subcontractor is subject to an enforceable written obligation to comply with the terms and conditions in this Attachment SCY. Within ten (10) days of DOHMH's request, the Contractor shall provide DOHMH with a copy of its contract with any Authorized Subcontractor.

(c) The Contractor shall be liable for the full or partial breach of any of the terms of this Attachment SCY by: **(A)** any of its subcontractors, whether or not an Authorized Subcontractor, or **(B)** any Person, whether or not an Authorized Person.

(d) The Contractor shall protect the privacy and security of DOHMH Data in accordance with the Agreement, industry best practices and all applicable laws, regulations and standards, including the Policies and Standards. Contractor shall implement, maintain and use appropriate administrative, technical and physical controls to ensure the SCIA of DOHMH Data, including, without limitation, to prevent the unauthorized, unlawful, or accidental use, destruction, alteration, disclosure, access, modification, or loss of DOHMH Data.

(e) Contractor shall not use DOHMH Data for any purpose other than to provide the Services to DOHMH.

(f) If Contractor is served with a Warrant, Subpoena, or any other order or request from a court or government body or any other person for any DOHMH Data, Contractor shall, as soon as reasonably practical and not in violation of any law, deliver a copy of such warrant, subpoena, order, or request to the Department.

17. INDEPENDENT REVIEW(S)/AUDIT(S)

(a) The Contractor shall engage a third-party internationally recognized auditor, at Contractor's own cost, to perform periodic audits, scans, and tests as follows:

( ) At least once per year and after any Security Incident that occurs during the Term:

(1) a SSAE 18/SSAE 16/SOC-1, Type II audit and a SOC-2, Type II audit of Contractor's controls and practices relevant to security, availability, Processing integrity, confidentiality and privacy of DOHMH Data;
(2) an audit pursuant to Contractor's information security program and practices;
(3) a network-level vulnerability assessment of all Contractor Systems used to deliver Services under the Agreement or to Process DOHMH Data; and
(4) a formal penetration test of all Contractor Systems used to deliver services under the Agreement or to Process Contract Data.

(ii) The Contractor shall provide Cyber Command with a copy of all unredacted reports generated for each audit, scan, and test within 10 days after its completion. Each report must: **(A)** indicate whether any material vulnerabilities, weaknesses, gaps, deficiencies, or breaches were discovered; and **(B)** if so, describe the nature of each vulnerability, weakness, gap, deficiency, or breach. The Contractor shall, at its own cost and expense, promptly remediate each vulnerability, weakness, gap, deficiency, or breach that is identified in a report.

THE CONTRACTOR SHALL PROVIDE CYBER COMMAND WITH COPIES OF REPORTS FROM ANY CYBERSECURITY AUDIT PERFORMED, WITHIN TWELVE (12) MONTHS OF EXECUTION OF THE AGREEMENT, BY THE CONTRACTOR OR BY A THIRD-PARTY AUDITOR AND ANY CYBERSECURITY AUDIT PERFORMED AFTER EXECUTION OF THE AGREEMENT WITHIN TEN (10) DAYS AFTER THE AUDIT'S COMPLETION.

18. NONCOMPLIANCE SELF REPORTING REQUIREMENT

The Contractor shall notify Cyber Command if at any time it is not in full compliance with any of the requirements of this agreement especially if Contractor makes any changes to the infrastructure of information systems that would affect DOHMH Data or result in noncompliance with any federal or state law, Policies and Standards, or terms of this agreement. Notification of each change shall be made to Cyber Command no later than thirty (30) business days after the change has occurred. For noncompliance, the Contractor shall submit to Cyber Command a document that includes the following:

(i) Date of discovery;
(ii) How the noncompliance was identified;
(iii) Nature of the noncompliance;
(iv) Scope of noncompliance; and
(v) Corrective actions with associated timelines.

19. VULNERABILITY REPORTING AND NOTIFICATION REQUIREMENT

The Contractor shall inform Cyber Command of any identified vulnerabilities in information systems no

later than ten (10) businesses days after receiving notification. The Contractor shall provide a report to Cyber Command that includes a detailed description of the identified vulnerabilities and a remedial plan with associated timelines informing DOHMH and Cyber Command of all actions the Contractor has taken or plans to take to rectify the vulnerabilities.

20. SUGGESTIONS

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

21. LIAISON

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

22. NO DOHMH DATA OUTSIDE UNITED STATES

The Contractor may not process, access, transfer, store, or export DOHMH Data outside the United States except with the express written permission of the Commissioner of DOHMH, and then only for the DOHMH Data specified in that permission.

23. INTEGRITY OF PUBLIC DOHMH DATA

The Contractor must use industry best practices to ensure that the value and state of all public DOHMH Data is maintained and that the public DOHMH Data is protected from unauthorized modification.

24. REMOTE ACCESS METHODS

The Contractor must obtain written permission from DOHMH for each method of remote access it wishes to use to access DOHMH Technology Assets.

25. WHAT TO DO IN CASE OF A SECURITY INCIDENT

(a) Contractor shall implement, maintain, test and update a Security Incident response plan. In the event of an actual or suspected Security Incident, Contractor shall:

( ) notify DOHMH and the NYC Cyber Command Citywide Security Operations Center ("**Cyber Command Citywide SOC**") by telephone at (718) 403-6761 within 24 hours.

(i) notify DOHMH and the Cyber Command Citywide SOC within 48 hours by written notice to SOC@cyber.nyc.gov, summarizing, in reasonable detail, the nature and scope of the Security Incident (including a description of all impacted DOHMH Data and DOHMH Technology Assets) and the corrective action already taken or planned by Contractor, which shall be timely supplemented to the level of detail reasonably requested by DOHMH, inclusive of relevant investigation or forensic reports.

(ii) promptly, at its own cost and expense, take all reasonable and necessary actions

to confirm, contain and end the Security Incident, mitigate its impact to DOHMH, and prevent recurrence.

(iii) not delete any impacted virtual/cloud instances or re-image any impacted systems without prior consultation and agreement with Cyber Command.

(iv) cooperate with DOHMH in the investigation of the Security Incident, including promptly responding to DOHMH's reasonable inquiries and providing prompt access to all evidentiary artifacts associated with or relevant to the Security Incident, such as relevant records, logs, files, data reporting, and other materials.

(v) permit DOHMH, in its sole discretion, to immediately suspend or terminate Contractor's right to create, process, access, transfer, store, or dispose of DOHMH Data or operate DOHMH Technology Assets.

(vi) not inform any third party that the Security Incident involves DOHMH Technology Assets or Data without first obtaining DOHMH's prior written consent, except to the extent required by law or by third parties engaged by the Contractor to remediate the Security Incident.

(vii) collaborate with DOHMH in determining whether to provide notice of the Security Incident to any person, governmental entity, the media, or other party, and the content of any such notice. DOHMH will make the final determination as to whether notice will be provided and to whom, the content of the notice, and which Party will be the signatory to the notice.

(viii) promptly notify DOHMH and the Chief Information Security Officer for the City of New York of any investigations of its data use, privacy or cybersecurity practices, or a Security Incident by a governmental, regulatory or self-regulatory body.

(ix) bear the responsibility and all related costs for any Security Incident to the extent that DOHMH is not at fault and caused by a vulnerability in the Contractor's product(s) or system(s), including the cost of any associated remedial actions or mitigation steps, consumer notification and related responses, credit monitoring, notification, regulatory investigations, fines, penalties, enforcement actions and settlements.

26. NOTIFICATION TO CYBER COMMAND

With the exception of the notification requirements applicable to a Security Incident as reflected in Section 25 of this Attachment, Contractor shall submit all notices, including any reporting documents, audit materials and other security documentation, to Cyber Command by email at compliance@cyber.nyc.gov.

27. MATERIAL BREACH

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

28. SECURITY INCIDENT RESPONSE CONTACTS

Contractor shall provide to DOHMH contact information for the Contractor's Chief Information Security Officer (CISO) or Senior Information Security Representative

29. SECURITY INCIDENT RESPONSE CONTACT: [NAME, TITLE, TELEPHONE NUMBER, EMAIL]
Contractor agrees to promptly notify DOHMH's CISO of any changes to this information.

30. 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.

[END OF ATTACHMENT SCY]

Version	**Date**
1.0	Pre 2023
2.0	October 2023