CLOUD SERVICES RIDER

This cloud services rider (the "Rider") is included in the ETL Proof of Concept Agreement and made a part thereof. In the event that the Parties pursue a paid procurement, such paid procurement will include the City's template cloud services agreement and expressly not this Rider.

1. DEFINITIONS. Capitalized or defined terms not expressly defined in this Rider have the meaning given to them in the Agreement.

1.1. "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, 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 one (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).

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

1.3. "City Systems" means any system owned, maintained or operated by or on behalf of the City that connects to a City network, enables operational functions of the City, or creates, processes, accesses, transfers, stores, or disposes of City Data.

1.4. "City Technology Assets" means all City facilities, City Systems, City telecommunications, electronic data created, processed, accessed, transferred, stored, or disposed of by City 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.

1.5. "Cloud Service/s" means the software-, platform-, infrastructure- or other "as a service" solution for which access is provided by Provider to the City under the Agreement, including any client software provided to the City by Provider for use with the Cloud Service. Any software to be installed on the City's hardware for the purpose of facilitating the City's use of the Cloud Services shall be deemed to be a part of the Cloud Services.

1.6. "Cyber Command" means the Office of Cyber Command, established within the New York City Office of Technology and Innovation ("OTI"), that is empowered to ensure compliance with Policies and Standards, mitigate cyber threats, mandate deployment of technical and administrative controls, review cyber related spending, and collaborate with federal and state government agencies and private sector organizations.

1.7. "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.

1.8. "DOITT" means the City Department of Information Technology and Telecommunications.

1.9. "Non-Public City Data" means all City Data that is considered Restricted or Sensitive Information as those categories are defined by the City's Policies and Standards. All Personal Identifying Information (as defined in Section 10-501 of the New York City Administrative Code or successor), Identifying Information (as defined in Section 23-1201 or successor), information protected from unauthorized use or disclosure by local, state or federal law and regulation, the City's confidential information (including information disclosed or made available by the City in the course of receiving maintenance, subscription and support and other services) and security information is Non-Public City Data.

1.10. "Open-Source Software" or "OSS" means an open source or other license that requires, as a condition of use, modification, or distribution, that any resulting software must be (a) disclosed or distributed in source code form; (b) licensed for the purpose of making derivative works; or (c) redistributable at no charge.

1.11. "Policies and Standards" means the Citywide Information Security Policies and Standards, Cyber Command Policies and Standards, or any other 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.

1.12. "PPB Rules" means the New York City Procurement Policy Board Rules.

1.13. "Provider Systems" means the facilities, systems, networks and IT environments that are used to Process any City Data, deliver any Cloud Services or to otherwise meet any of Provider's obligations under the Agreement. For the purposes of this definition, "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.

1.14. "Security Incident" means an event that compromises or is suspected to compromise the security, confidentiality, availability or integrity of City Data, City Technology Assets or Provider Systems, including by compromising the physical, technical, administrative or organizational safeguards implemented by Provider to protect the security, confidentiality, availability or integrity of City Data, City Technology Assets or Provider Systems. Examples of a Security Incident include, but are not limited to, the unauthorized acquisition or use of unencrypted City Data (or encrypted City Data and the decryption key), network intrusions, ransomware infections, a breach of access credentials and DoS attacks.

2. LICENSE AND USE

2.1 Authorized User. The authorized user of the Cloud Service is the City, including its employees, authorized agents, consultants, auditors, other independent providers and any external users contemplated by the Parties. This paragraph does not modify the quantity of users permitted to use the Cloud Service.

3. DATA MANAGEMENT AND SECURITY

3.1 Safeguards to Protect City Data. Provider shall implement and maintain appropriate physical, technical, administrative, and organizational safeguards in accordance with industry best practices and applicable law to protect the security, confidentiality, availability, and integrity of City Data, including, but not limited to, the safeguards described in this Agreement.

3.2 Backup and Recovery of City Data. As a part of the Cloud Services provided under this Agreement, Provider is responsible for creating, maintaining, and testing backup copies of City Data. Provider is responsible for an orderly and timely recovery of the Cloud Services and City Data in the event that the Cloud Services are interrupted. Except when shorter time(s) are otherwise provided in a separate agreement, the recovery time objective ("RTO") for Cloud Services is six (6) hours and the recovery point objective ("RPO") for City Data is two (2) hours. For the purpose of calculating the RTO, recovery time is equal to the elapsed period of time between the commencement of an interruption and the time at which the Cloud Service is fully restored and available for use by the City. RPO means the period of time during which changes made to data shall not be included in a replication or other backup copy. Provider shall replicate data to a disaster recovery site that meets the requirements in this Agreement. Provider shall maintain no less than thirty (30) days of backups. Any backups of City Data shall not be considered in calculating storage used by the Department.

3.3 Disaster Recovery Sites. Provider shall have a minimum of one (1) disaster recovery site at a distance of at least five hundred (500) miles from the primary site. City Data must be replicated from the primary data center to the disaster recovery site in a time and manner sufficient to meet the RPO, and the Cloud Service must be configured to fail over from the primary data center to the disaster recovery site within the RTO. The disaster recovery site must be capable of supporting the Cloud Service at full load. The Department and City shall not incur any costs in relation to additional recovery site(s).

3.4 Disaster Recovery Plans. Provider shall implement, maintain, and test disaster recovery plans to minimize downtime resulting from all hazards, including system failure. Provider represents that these disaster recovery plans are documented, tested no less frequently than once every twelve (12) months, and updated as required. The City has a right to review Provider's disaster recovery plans, and Provider must, upon the City's request, provide the Department with a copy of such plans.

3.5 Data Availability, Storage, and Retention. Provider shall comply with the following:

3.5.1 Provider shall ensure that all City Data is available to the Department at all times (24/7/365) during the term of the Cloud Services and for a period of ninety (90) days after the term ends, including during any suspension of Cloud Services.

3.5.2 All City Data uploaded by the City and stored by Provider shall be available to the City to copy back to the City's storage without alteration or loss and at no additional charge.

3.5.3 Provider may not use, access, or perform any analytical analyses of any kind on data derived from the City's usage of the Cloud Service, whether anonymized or aggregated or both, except as agreed to in writing by the City in its discretion, or as required for Provider to provide the Cloud Service.

3.5.4 City Data shall not be altered, moved, or deleted without the Department's consent.

3.5.5 If legal mandates for data retention apply specifically to City Data, Provider shall comply with all such mandates communicated to Provider in writing.

3.5.6 Provider agrees that City Data shall remain in the United States.

3.6 Forensic and Investigative Response. Provider must document and maintain appropriate chain of custody throughout the duration of this Agreement for the purposes of potential forensic or legal investigation. Provider shall not remove metadata, except as directed by Department.

3.7 Access to City Data. Provider shall implement identity and access control policies and procedures in accordance with applicable law and industry best practices, and as approved by the City. Upon the request of the City, Provider shall support federated identity and access management.

3.8 Occurrences Affecting City Data. Provider shall implement, maintain, test and update an incident response plan in accordance with applicable law and industry best practices. Provider represents that (a) prior to the execution of this Agreement, Provider has provided the City with a copy of its current written incident response plan, and (b) on an annual basis thereafter, Provider shall provide the City with its current written incident response plan.

3.9 Security Incident. In the event of a Security Incident, Provider shall:

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

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

3.9.3 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 the City, and prevent recurrence.

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

3.9.5 cooperate with the City in the investigation of the Security Incident, including promptly responding to the City'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.

3.9.6 permit the City, in its sole discretion, to immediately suspend or terminate Provider's right to create, process, access, transfer, store, or dispose of City Data or operate City Technology Assets.

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

3.9.8 collaborate with the City 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. The City 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.

3.9.9 in the case of Protected Health Information or Electronic PHI ("**PHI/e-PHI**"), as defined in 45 CFR §160.103, or in the case of Personal Identifying Information, as defined in Section 10-501(a) or its successor of the Administrative Code of the City of New York ("**PII**"), at the City's request and pursuant to the City's express instructions as to form, content, scope, recipients, and timing, notify the affected individuals as soon as practicable but no later than required to comply with applicable law.

3.9.10 in the case of PHI/e-PHI or PII, provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required period for monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

3.9.11 bear the responsibility and all related costs for any Security Incident to the extent that the City is not at fault or caused by a vulnerability in the Provider'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.

3.9.12 promptly notify the City of any investigations of its data use, privacy or cybersecurity practices, or a Security Incident by a governmental, regulatory or self-regulatory body.

3.10 Termination for Security Incident. In the event of a Security Incident that is caused by Provider's failure to comply with this Agreement, the Department may terminate the Cloud Services on no less than fifteen (15) days' prior written notice. The consequences under Section 15.4 shall apply.

3.11 Notice in Event of Provider Receipt of Warrant, Subpoena, or other Governmental Request. If Provider is served with a warrant, subpoena or any other order or request from a court or government body or any other person for any City Data, Provider shall, as soon as reasonably practical and not in violation of law, deliver a copy of such warrant, subpoena, order, or request to the Department.

3.12 Data Commingling. Provider shall not commingle City Data with non-City Data that is uploaded by Provider, its customers or other third parties and stored by Provider. Provider shall provide the City with details of how it performs data segregation.

4. DATA PRIVACY AND INFORMATION SECURITY PROGRAM

4.1 Provider Privacy and Security Program. Without limiting Provider's obligation of confidentiality, as further described in the Agreement, Provider shall be responsible for establishing and maintaining a data privacy and information security program ("Privacy and Security Program") that includes reasonable and appropriate physical, technical, administrative, and organizational safeguards, to: (a) ensure the security, confidentiality, availability, and integrity of City Data; (b) protect against any anticipated threats or hazards to the security, confidentiality, availability, or integrity of City Data; (c) protect against unauthorized or illegal or accidental disclosure, access to, destruction, alteration, modification, loss, acquisition or use of City Data; (d) ensure the proper disposal of City Data, if requested by the City or required by applicable law; and, (e) ensure that all employees, agents, third party providers, and subcontractors of Provider comply with all of the foregoing. Provider shall submit its Privacy and Security Program to the City, and in no case shall the safeguards of such Privacy and Security Program be less stringent than the safeguards used by the City, or such other safeguards as shall be approved by Citywide Chief Information Security Officer in writing.

4.2 Security Controls. Provider's privacy and security controls must include, but not be limited to, physical, administrative, software, and network security measures, employee screening, employee training and supervision, and appropriate agreements with employees and subcontractors.

4.3 Requirements for Systems Providing Critical Functions. Provider shall provide the City 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. Provider shall ensure that all necessary capabilities and equipment potentially required to service critical technology in the event of an incident is locally available.

4.4 Treatment of City Data. Provider understands and acknowledges that the City may not be in compliance with nor subject to the General Data Protection Regulation (EU) 2016/279 and its implementing regulations.

4.5 Privacy and Security Audit.

4.5.1 Privacy and Security Audit by Provider. No less than annually, Provider shall conduct a comprehensive audit of its Privacy and Security Program and provide such audit findings to the City.

4.5.2 Independent Audit. In addition to the audit required by Section 4.5.1 above, Provider shall engage a third-party internationally recognized auditor (the "Auditor"), at Provider'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 and at the request of the Department:

4.5.2.1 a SSAE 18/SSAE 16/SOC-1, Type II audit and a SOC-2, Type II audit of Provider's controls and practices relevant to security, availability, integrity, confidentiality and privacy of City Data;

4.5.2.2 a network-level vulnerability assessment of all Provider systems used to deliver Cloud Services; or

4.5.2.3 risk assessment, which may include but is not limited to a formal penetration test of all systems used to deliver Cloud Services; or

4.5.2.4 ISO 27001 audit (most current version) and Provider's controls and practices relevant to security, availability, integrity, confidentiality and privacy of City Data.

4.5.3 Privacy and Security Audit by City. Without limiting any other audit rights of the City, the City shall have the right to review and audit Provider's Privacy and Security Program and/or IT infrastructure and information security controls and processes prior to the commencement of this Agreement and from time to time during the term of this Agreement. The City reserves the right to also perform relevant tests to ensure Provider is compliant with required security policies and standards. Provider shall permit the City to perform such audit, including an audit of the physical security of any of Provider's premises applicable to the Cloud Services provided to the City and shall fully cooperate and furnish all requested materials in a timely manner. The review and audit may be conducted remotely or onsite by the City or a City provider and at the City's expense. The City shall conduct on-site audits in a manner so as not to unreasonably interfere with Provider's business operations. In lieu of an on-site audit, upon request by the City, Provider shall complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by the City regarding Provider's Privacy and Security Program.

Provider shall not be entitled to compensation from the City for the time it spends cooperating with any of the audits, scans, or tests provided for in this Section 4.5.3, or in completing any audit questionnaire(s).

4.5.4 Findings. Provider shall provide the City with a copy of all reports generated for each audit, scan, and test within ten (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. Provider shall, at its own cost and expense, promptly remediate each vulnerability, weakness, gap, deficiency, or breach that is identified in a report and provide the City with documentation of the remedial efforts within ten (10) days after their completion.

4.5.5 Performance Testing. Performance testing is required for all public-facing applications. Provider must demonstrate the ability to conduct performance testing and establish terms for testing and cost.

4.6 Logs. Provider must generate, maintain, constantly monitor, and analyze security audit logs that contain the information as specified in NIST Special Publication 800-92. If requested by the City, Provider shall provide the audit logs to the City in a format agreed upon by both parties.

4.7 Vulnerabilities. Provider's software applications and any third-party software applications embedded in Provider's software applications must be free from vulnerabilities and defects. Provider must conduct vulnerability scanning for critical systems or systems hosting sensitive data as often as required by law, relevant policy, to maintain certification(s), and in response to the Department of Homeland Security's critical vulnerability/patch publication(s). Provider must provide attestation by an objective third party, stating that the application has been tested for known security vulnerabilities, including, without limitation, those listed in the "OWASP Top-10" as published by the Open Web Application Security Project (see www.owasp.org for current list of the top 10), NIST 800-53 and the NIST Cybersecurity Framework (CSF). If requested by the City, Provider shall also provide the City with information about whether it patched critical vulnerabilities and the remediation steps it took.

4.8 Vulnerability Reporting and Notification Requirement. Provider shall inform the City and Cyber Command of any identified vulnerabilities in information systems no later than ten (10) business days after receiving notification. Provider shall provide a report to the City and Cyber Command that includes a detailed description of the identified vulnerabilities and a remedial plan with associated timelines informing the City and Cyber Command of all actions Provider has taken or plans to take to rectify the vulnerabilities.

4.9 Authorization and Access. Provider's access controls must enforce the following information technology security best practices with respect to its services:

4.9.1 Least Privilege. Provider shall authorize access only to the minimum amount of resources required for a function.

4.9.2 Separation of Duties. Provider shall divide functions among its staff members to reduce the risk of one person committing fraud undetected.

4.9.3 Role-Based Security. Provider shall restrict access to its services to only authorized users. Provider shall base access control on the role a user plays in an organization.

4.9.4 If not utilizing single sign on and Provider's previously authorized resource should no longer have authorization/ access, Provider shall immediately revoke authorization. Provider shall periodically scan for dormant accounts and expeditiously remove/deactivate.

4.10 Change in Service. Provider shall notify the Department of any enhancement, upgrade, or other change in the Cloud Service that may impact the security, availability, or performance of the Cloud Services.

5. VENDOR INDUCED INHIBITING CODE, HARDSTOP/PASSIVE LICENSE MONITORING, MALWARE AND OTHER DESTRUCTIVE MECHANISMS

5.1 Provider shall not include any vendor induced inhibiting code ("VIIC") or any other inhibitor in the Cloud Services or on reports and data submitted and provided to the City. VIIC means any deliberately included application or system code that shall degrade performance, result in inaccurate data, deny accessibility, or adversely affect, in any way, programs or data or use of the Cloud Services. Provider warrants that (a) the Cloud Services contain no destructive programming that is designed to permit Provider or third parties unauthorized access to, or use of, the City's systems or networks, or would have the effect of disabling or otherwise shutting down all or any portion of the Cloud Services, and (b) the Cloud Services shall contain no viruses, Trojan Horses, worms, spyware, malware, or any other form of malicious code.

6. ENCRYPTION AND AUTHENTICATION

6.1 Provider shall encrypt all City Data, including backups, while at rest and in transit from end to end using encryption standards and methods that are approved and recommended by the National Institute of Standards and Technology ("NIST") and, as applicable, FIPS 140-1 and FIPS 140-2 or their successors.

6.2 The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of Provider and approved in writing by the Chief Information Security Officer for the City of New York. Proven algorithms such as those approved by NIST as listed in their Cryptographic Standards and Guidelines, or as defined in the NYC Encryption Standard must be used as the basis for encryption technologies. Algorithms must be implemented in a secure manner, as defined by NIST in their Cryptographic Standards and Guidelines, or as defined in the NYC Encryption Standard.

6.3 For password hashing, PBKDF2, Scrypt and Bcrypt or better must be used. Approved encryption algorithms must be of a minimum key length of 128 bits.

6.4 Shared keys used for IPSec tunnels must be complex, randomly generated pursuant to Section 6.5, and not be stored for later reference. During initial setup of an IPSec tunnel, the shared key must be transmitted out of band to the other party involved. Provider must utilize cryptographic algorithms that are acceptable to the City.

6.5 Random number generation shall be compliant with NIST SP 800-90A and FIPS 140-2. Furthermore, it shall meet the requirements of the draft NIST SP 800 90B and C. NIST resources are available at https://csrc.nist.gov/.

6.6 Digital Certificates that validate and secure communications used by the general public must be generated by trusted third-party providers. Certificates that validate communications used by internal City of New York employees or business partners and/or web applications can be generated by the Citywide CITYNET Certificate Authority (internal PKI) or third-party providers. DOITT is responsible for managing and operating Citywide CITYNET Certificate Authority. For internal City of New York namespaces, DOITT must generate digital certificates through the Citywide Certificate Authority (internal PKI), whereas for external namespaces trusted third-party providers must be used.

7. CITY SECURITY REVIEW OF PROVIDER'S CLOUD SERVICES / SOFTWARE SECURITY ASSURANCE (SSA) APPROVAL

7.1 The Cloud Services may be subject to a security review by the City. If such a security review has been completed and the City's written disposition requires Provider to comply with the City's prescribed security measures ("City Security Measures"), then, in addition to complying with this Agreement, Provider shall comply with the City Security Measures.

7.2 Any written disposition of a security review by the City shall not be deemed to constitute an endorsement of the Cloud Services or a certification that the Cloud Services meet the City Security Measures or the requirements under this Agreement. Provider remains fully responsible for ensuring compliance with the City Security Measures and this Agreement. At all times during the term of the Cloud Services, Provider agrees to cooperate with the City to ensure that Provider is in compliance with all City Security Measures and the provisions of this Agreement.

7.3 Following the review and written disposition described in Sections 7.1 and 7.2 above, Provider agrees to (a) if required by Cyber Command, submit information into the SSA tool, and (b) submit all devices, applications, systems, software and infrastructure used to support City systems to the City's applicable security testing process. The City's security testing process may include a formal application scan (in staging) and/or a penetration test of Provider's Cloud Services and any required remediation. Provider understands and acknowledges that failure to meet the City's security requirements is a material breach of this Agreement.

7.4 Prior to any application scan or penetration test, Provider shall execute any waiver that may be required by the City.

8. DATA OWNERSHIP

8.1 The City retains sole ownership and Intellectual Property Rights in and to all City Data. Provider shall not use the City Data for any purpose other than as required to provide the Cloud Services to the Department.

8.2 Except as provided in Section 10.4, Provider shall not retain any City Data after a ninety (90) day period following the expiration/termination of the term or following the City's request pursuant to Section 10.1.1.

8.3 The City hereby retains all right, title, and interest in and to any suggestion, enhancement request, recommendation, correction or other feedback provided to Provider relating to Provider's Cloud Services, except that Provider may use such information in connection with its provision of Cloud Services to the City. Any feedback from the City is provided "as is", and the City disclaims any and all warranties whatsoever.

8.4 Except as expressly provided in this Agreement, no ownership right or license to use, sell, exploit, copy or further develop City Data, any confidential information or Intellectual Property of the City is conveyed to Provider.

9. NO SUPPLEMENTARY AGREEMENTS OR TERMS; NO UNILATERAL CHANGES; APPLICABILITY.

9.1 All click-through, click-wrap, or shrink-wrap agreements or other end user terms and conditions that are embedded in or provided with any of Provider's Cloud Services or presented to users in the course of the Department's use of the Cloud Services are not applicable to the City, even if use of Provider's Cloud Services require an affirmative acceptance of those terms. The terms and conditions of this Agreement are in static form, and no online terms and conditions that are incorporated by reference in this Agreement or set forth in hyperlinked websites are binding on the City, including any other privacy policies of Provider and third-party providers.

10. SEPARATION ASSISTANCE

10.1 In the event of impending or actual separation and for up to ninety (90) days following such expiration or termination, the Department may request in writing that Provider do or permit the City to do any of the following, or any combination of the following:

10.1.1 Export and/or copy City Data, subject to any applicable charges as provided in this Agreement. If the Department requests an export of City Data, such exported data shall be in a format approved by the Department in writing.

10.1.2 Destroy any City Data. Any written request by the Department directing Provider to destroy City Data shall specify what data the Department is requesting to be destroyed. Except for actions required by this Agreement, Provider shall not destroy any City Data in the absence of a specific written request from the Department. If Provider destroys any City Data, it shall verify such destruction in writing. Destruction of City Data shall be performed by Provider in a manner that complies with NIST and precludes recovery or reconstruction of such data by all currently known methods and technology. Unless otherwise specified by the City, a request to destroy City Data includes destruction of live/production data as well as data housed as/in backup(s).

10.1.3 When applicable, upon the City's request, Provider shall verify it has turned off the City's access to the Cloud Services.

11. RECORDS AND AUDIT

11.1 Records. Provider agrees to maintain separate and accurate books, records, documents and other evidence ("books and records"), and to utilize appropriate accounting procedures and practices in the performance of this Agreement. Provider agrees to retain all books and records, relevant to this Agreement, including those required pursuant to the foregoing sentence for six (6) years after the final payment or expiration or termination of this Agreement, or for a period otherwise prescribed by law, whichever is later. In addition, if any litigation, claim, or audit concerning this Agreement has commenced before the expiration of the six (6)-year period, the records must be retained until the completion of such litigation, claim, or audit.

11.2 Audit by City. This Agreement and all books and records required to be maintained or retained pursuant to this Agreement, including all vouchers or invoices presented for payment and the books and records upon which such vouchers or invoices are based (e.g., reports, cancelled checks, accounts, and all other similar material), are subject to audit under applicable law by (a) the City, including the New York City Comptroller (the "Comptroller"), the Department, and the Department's Office of the Inspector General, (b) the State, (c) the federal government, and (d) other persons duly authorized by the City. Provider shall submit any and all documentation and justification in support of expenditures or fees under this Agreement as may be required by the Department and by the Comptroller in the exercise of his or her powers under law.

12. ADDITIONAL SECURITY REQUIREMENTS

12.1 Citywide Information Security Policy. Provider shall comply with the Policies and Standards. In addition, Provider shall ensure that all subcontractor(s) approved by the City in writing (each an "Authorized Subcontractor") and any employee of Provider or an Authorized Subcontractor who needs to know the City Data in order to perform Provider's obligations (each an "Authorized Person") who may have access to any City Data or City Technology Assets in the course of carrying out their responsibilities or job functions comply with this Section 14.1. Provider shall be liable for the breach by an Authorized Subcontractor or Authorized Person or any of its subcontractors or persons who are not considered Authorized Subcontractors or Authorized Persons.

12.2 DOITT User Responsibility Policy ("URP"). Provider shall require each Authorized Person who may have access to any City Technology Assets to sign a written acknowledgement and agreement to comply with its terms prior to his or her assignment to perform any Services pursuant to this Agreement. Provider shall provide a signed copy of the URP acknowledgement for each Authorized Person to the City project manager, or a person designated by the City, within fifteen days (15) days after the Authorized Person is assigned to perform Services pursuant to this Agreement.

12.3 Non-Disclosure Agreement. If requested by the City, Provider shall require its Authorized Subcontractors and Authorized Persons who either work in direct support of the Cloud Services or who may reasonably be anticipated to receive City Data to execute a Non-Disclosure Agreement in a form acceptable to the City.

12.4 Provider Security Questionnaire. Provider shall complete and respond to all security questionnaires from the City within thirty (30) business days.

12.5 Noncompliance Self Reporting Requirement. Provider shall notify the Department and Cyber Command of any changes to the infrastructure of all information systems that would affect City Data or result in noncompliance with any federal or state law, Policies and Standards, of terms of this Agreement. Notification of each change shall be made to the City and Cyber Command no later than three (3) business days after the change has occurred. For noncompliance, Provider shall submit to Cyber Command a document that includes the following: (a) date of discovery; (b) how the noncompliance was identified; (c) nature of the noncompliance; (d) scope of noncompliance; and (e) corrective actions with associated timelines.

12.6 Remote Access Methods. Provider must obtain written permission from the City for each instance of remote access it wishes to use and access City Technology Assets.

13. GENERAL

13.1 Order of Precedence. This Rider takes precedence over any provision in the Agreement. In the event of a conflict between this Rider and the Agreement, this Rider shall prevail.

13.2 Survival. All terms of this Rider that should by their nature survive termination shall survive, including, Section 3 (Data Management and Security), Section 4 (Data Privacy and Information Security Program), Section 13.3 (Limitation of Liability), Section 13.4.1 (Intellectual Property), and Section 13.5 (Indemnification).

13.3 Limitation of Liability. Subject to the provisions of Section 13.3.2 below, each Party's aggregate liability for all claims arising out of the Cloud Services, whether in contract, tort or otherwise, shall not exceed one million dollars ($1,000,000). The limitation of liability set forth herein shall not apply to Provider's liability arising out of any of the following: (a) Provider's indemnification obligations under this Rider; (b) Provider's breach of the confidentiality provisions in the Agreement; (c) Provider's breach of Section III (Data Management and Security) or Section IV (Data Privacy and Information Security Program) of this Rider, (d) the infringement by Provider, or any of its Affiliates or subcontractors, of the Intellectual Property of the City or of a third party; and (e) to the extent prohibited by law. Any provision in the any other agreement limiting or disclaiming Provider's liability is hereby deemed to be void and unenforceable.

13.4 Warranties and Representations.

13.4.1 Intellectual Property. Provider represents and warrants that it has the rights necessary to provide the Cloud Services to the City in accordance with this Agreement.

13.4.2 Additional Warranties and Representations. Provider further represents and warrants that: (a) the Cloud Services shall be provided in a professional, competent, and timely manner by appropriately qualified personnel in accordance with this Rider and consistent with Provider's best practices; (b) Provider shall provide adequate training, as needed, to the Department on the use of the services; (c) the Cloud Services shall comply with all applicable international, federal, state, and local laws, rules, and regulations, including but not limited to laws relating to privacy, security, and anti-corruption; (d) the Cloud Services do not and shall not infringe the Intellectual Property Rights of any third party; (e) the Cloud Services are compatible and shall maintain compatibility with third-party software, including any OSS; and (f) there is no pending or threatened litigation involving Provider that may impair or interfere with the Department's right to use the services.

13.5 Indemnification.

13.5.1 Provider's Indemnity. Provider shall defend, indemnify and hold the City and its employees, officers, and agents (collectively, "Indemnitees") harmless from any and all judgments, damages, liabilities, amounts paid in settlement, awards, fines, penalties, disbursements , costs and expenses (including witness fees, expert fees, investigation fees, travel expenses, bonds, the cost of establishing the right to indemnification under this Section 16.6.1, court or arbitration costs and reasonable attorney's fees) to which the Indemnitees may be subjected, become liable to pay, suffer or incur in connection with any claim, allegation, suit, subpoena, action or proceeding (whether completed, actual, pending, threatened, civil, criminal, investigative, administrative, meritorious or without merit) that arises from or relates to (a) breach of confidentiality; (b) costs and expenses to which the Indemnitees may suffer in connection with any operations of Provider and/or its subcontractors to the extent resulting from any negligent act of commission or omission,

any intentional tortious act; (c) failure to comply with the provisions of this Agreement (including but not limited to a breach of representations and warranties) or of the law; and (d) the infringement of any copyright, trade secret, trademark, patent or other tangible or intangible property or personal right of any third party by Provider or its subcontractors. Provider shall defend, indemnify and hold the Indemnitees harmless regardless of whether or not the alleged infringement arises out of the use of the Cloud Service in a manner not expressly contemplated in this Agreement, or in combination with any hardware, equipment or other software not provided or authorized by Provider. Insofar as the facts or the law relating to any claim would preclude the Indemnitees from being completely indemnified by Provider, the Indemnitees shall be partially indemnified by Provider to the fullest extent permitted by law.

13.5.2 Indemnification for Security Incidents. Provider shall defend, indemnify and hold Indemnitees harmless from any and all costs and expenses arising out of a Security Incident.

13.5.3 No Indemnification by the City. Any provision in any separate agreement requiring the City to provide indemnification is hereby deemed to be void and unenforceable.

13.6 Use of Third-party Providers.

13.6.1 Provider must identify any third-party entities involved in the provision of the Cloud Service and provide the Department with a copy of Provider's agreement with the third-party provider. The agreement must be approved in writing by the City. Provider shall notify the Department in the event that Provider makes any change in the list of third-party providers that it uses prior to making any change along with a copy of any applicable terms. Notwithstanding the City's approval of such third-party provider agreements, (a) Provider shall remain responsible for any and all performance required under this Agreement, including, but not limited to, the obligation to properly supervise, coordinate, and perform, all work required hereunder, and no third-party provider agreement shall bind the City; and (b) Provider shall ensure that any third-party provider complies with the requirements in this Agreement, including the minimum service levels set forth in the SLA. If Provider proceeds with an unapproved third-party provider, it shall be deemed liable to the City for any third-party claims to the same extent as the third-party provider would have been liable had it agreed to the terms set forth in this Agreement.

13.6.2 Any subcontractor or affiliate (as defined below) of Provider that provides any software or services in connection with the Cloud Services is deemed to be a subcontractor whose subcontracts must be approved in writing by the City. As used in this paragraph, "affiliate" means any parent, subsidiary or other entity that is (directly or indirectly) controlled by, or controls, Provider. Any provision in this Rider to the contrary is deemed to conflict with this Rider.

13.7 Fees.

13.7.1 The City is not responsible for an early termination fee.

13.7.2 The City shall not be liable for any unauthorized use, including fees and charges that may become due to Provider as a result of that use.

13.8 Insurance. In addition to any insurance requirements set forth in the Rider, Provider shall comply with the requirements of this Section.

13.8.1 Data Breach and Privacy Cyber Liability. Provider shall maintain at all times during the provision of Cloud Services, and as otherwise required herein, data breach and privacy cyber liability insurance with limits of no less than $1,000,000 per claim and $2,000,000 in the aggregate. This policy must include coverage for:

13.8.1.1 failure to protect confidential information, including personally identifiable information;

13.8.1.2 failure of the security of Provider's computer systems;

13.8.1.3 failure of the security of the City's systems or City Data due to the actions or omissions of Provider;

13.8.1.4 Data breach expenses, including forensic services, the cost of complying with privacy laws and regulations, cost of undergoing regulatory examinations and defending regulatory actions, including legal representation, cost of internal investigation to determine the cause of the breach, notification costs, public relations and crisis management costs, credit monitoring, fraud consultation, credit freezing, fraud alert, and identity restoration services;

13.8.1.5 Costs arising from cyber extortion threats, including the payment of ransom demands;

13.8.1.6 The alteration, loss, corruption of data, including costs to recover, correct, reconstruct, and reload lost, stolen, or corrupted data;

13.8.1.7 The cost of replacing, repairing, or restoring computer systems, including hardware (including laptops and mobile devices), software, networking equipment, and storage;

13.8.1.8 Costs arising from an attack on a network or computer system, including denial of service attacks, malware, and virus infections;

13.8.1.9 Dishonest, fraudulent, malicious, or criminal use of a computer system by a person, whether identified or not, and whether acting alone or in collusion with other persons;

13.8.1.10 media liability; and

13.8.1.11 Cyber theft of customer's property, including but not limited to money and securities.

13.8.2 Technology Errors and Omissions. Provider shall maintain at all times during the provision of Cloud Services, and as otherwise required herein, technology errors and omissions insurance covering Provider in the amount of at least $1,000,000 per occurrence and $2,000,000 in the aggregate for damages arising from computer related services, including, but not limited to, one or any combination of the following: (a) consulting, (b) data processing, (c) programming, (d) system integration, (e) hardware development, (f) software development, (g) installation, (h) distribution or maintenance, (i) systems analysis or design, (j) training, (k) staffing or other support services, (l) cloud computing services, and (m) any electronic equipment, computer software developed, manufactured, distributed, licensed, marketed or sold. This policy must include coverage for third-party fidelity, including cyber theft.

13.9 Open-Source Software. If the Cloud Services consist of any Open-Source Software, Provider shall, upon request, furnish the Department with the applicable OSS licensing terms (the "Licensing Terms"). Provider shall be responsible for all third-party software and OSS incorporated in the Cloud Services. If the Cloud Services do not utilize any OSS, Provider shall affirm such in writing to the Department in advance of its processing of any order for such Cloud Services.

13.10 Cumulative Remedies; No Waiver. All rights and remedies whether conferred in this Rider, or by any other instrument or law shall be cumulative and may be exercised singularly or concurrently. The failure of any Party to enforce any of the provisions hereof shall not be construed to be a waiver of the right of such Party thereafter to enforce such provisions.

13.11 Notices. Provider shall submit notices as required in this Rider as set forth in the Agreement and as follows:

To Cyber Command regarding Security Incidents: soc@cyber.nyc.gov, soc@oti.nyc.gov, vuln@cyber.nyc.gov and 718-403-6761

To Cyber Command regarding anything other than Security Incidents: CISO@oti.nyc.gov

[REMAINDER OF PAGE INTENTIONALLY BLANK]