CLOUD AGREEMENT

TERMS AND CONDITIONS FOR CLOUD SERVICES

This Cloud Services Agreement ("**Agreement**"), made effective on date _________________ ("Effective Date"), is by and between _______________________, as the Cloud Service provider ("**Provider**"), and the City of New York through its Department of Health and Mental Hygiene ("DOHMH"), and are applicable to hosted services from Provider, including, but not limited to, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and software sold, licensed, transferred or otherwise provided to DOHMH by Provider or through a third-party reseller ("**Reseller**"). As used in this Agreement, "**Party**" refers to DOHMH or Provider (i.e., does not include a Reseller, if any) individually, and "**Parties**" means DOHMH and Provider, collectively.

WHEREAS,

I. DEFINITIONS

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. "**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.

1.3. "**DOHMH Data**" means information (including electronically stored information), databases, data compilations, reports, charts, graphs, diagrams, or other information created, generated or maintained by Provider or its subcontractors for the benefit of DOHMH under this Agreement, or made accessible by DOHMH to Provider under this Agreement or supplied, or derived from data supplied, to Provider or its subcontractors by or on behalf of DOHMH and any copies of such. For the avoidance of doubt, DOHMH Data includes but is not limited to data created solely by DOHMH's use of Provider's Cloud Services. DOHMH Data further includes all information that is considered Restricted or Sensitive Information as those categories are defined by DOHMH's Policies and Standards. All private 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, DOHMH's confidential information (including information disclosed or made available by DOHMH in the course of receiving maintenance, subscription and support and other services) and security information is DOHMH Data.

1.4. "**DOHMH Information Assets**" means all DOHMH Facilities, computer systems, electronic data stored, processed, transmitted, or printed by DOHMH computer systems, and such systems' peripheral equipment, networks, or magnetic data, as well as any cloud computing system utilized or leveraged by DOHMH or any non-DOHMH entity for DOHMH's use, and any electronic data stored, processed, transmitted, or printed by such system.

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

1.6. "**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.

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

1.8. "**Intellectual Property Rights**" or "**Intellectual Property**" means all proprietary information, patents, patent applications, trademarks, trade names, service marks, certification marks, collective marks, designs, processes, inventions, licenses, copyrights, and trade secrets of either Party, including, but not limited to, such rights relating to the origin, design, manufacture, programming, operations, function, configuration, or service of the licensed product.

1.9. "Internet of Things (IOT) Devices" mean interconnected devices that communicate and interact with each other, regardless of whether the devices connect directly to the internet or through other means such as local networks or private communication channels.

1.10. "**NYC3**" means the New York City Office of Cyber Command, which is part of the City.

1.11. "**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.

1.12. "**Policies and Standards**" means the Citywide Information Security Policies and Standards, Cyber Command Policies and Standards, or any other policies and procedures by NYC3 and OTI, available at https://www.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.

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

1.14. "**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.

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

1.16. "**Security Incident**" means any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, availability or integrity of

DOHMH Data, DOHMH Information 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 DOHMH Data, DOHMH Information Assets or Provider 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), network intrusions, ransomware infections, a breach of access credentials and DoS attacks.

II. LICENSE AND USE

2.1. License Grant. Subject to the terms and conditions of this Agreement, Provider grants DOHMH a worldwide, limited, non-exclusive right and license during the term of this Agreement: (a) to use the Cloud Services; (b) implement, configure and access the Cloud Services, including all actions and licenses necessary to fully effectuate the purposes of this Agreement and DOHMH's internal business and IT purposes; and (c) access and use Provider's documentation.

2.2. Authorized User. The authorized user of the Cloud Service is DOHMH, 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.

III. DATA MANAGEMENT AND SECURITY

3.1. Safeguards to Protect DOHMH 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 DOHMH Data, including, but not limited to, the safeguards described in this Agreement.

3.2. Backup and Recovery of DOHMH Data. As a part of the Cloud Services provided under this Agreement, Provider is responsible for creating, maintaining, and testing backup copies of DOHMH Data. Provider is responsible for an orderly and timely recovery of the Cloud Services and DOHMH 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 DOHMH 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 DOHMH. 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 DOHMH Data shall not be considered in calculating storage used by DOHMH.

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. DOHMH 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. DOHMH 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. DOHMH has a right to review Provider's disaster recovery plans, and Provider must, upon DOHMH's request, provide DOHMH 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 DOHMH Data is available to DOHMH 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 DOHMH Data uploaded by DOHMH and stored by Provider shall be available to DOHMH to copy back to DOHMH'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 DOHMH's usage of the Cloud Service, whether anonymized or aggregated or both, except as agreed to in writing by DOHMH in its discretion, or as required for Provider to provide the Cloud Service.

3.5.4. DOHMH Data shall not be altered, moved, or deleted without DOHMH's consent;

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

3.5.6. Provider agrees that DOHMH 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 DOHMH.

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

3.8. Occurrences Affecting DOHMH 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 DOHMH with a copy of its current written incident response plan, and (b) on an annual basis thereafter, Provider shall provide DOHMH with its current written incident response plan. Except as required by applicable law without the possibility of contractual waiver, Provider shall not inform any third party of any Security Incident in the absence of DOHMH and NYC3's prior written authorization to make the disclosure. DOHMH and NYC3 shall determine whether notice is required to be provided to individuals, regulatory and law enforcement agencies or any other third party and whether any remediation may be offered to individuals affected by the Security Incident.

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

3.9.1. notify DOHMH and NYC3 as soon as possible, but in no event later than twenty-four (24) hours after discovery of the Security Incident, informing DOHMH of the nature of the Security Incident, the harmful effects of which Provider is aware, and all actions Provider has taken and plans to take. For purposes of this section, a Security Incident is deemed to be discovered as of the first day on which it is known by Provider, its employees, subcontractors or other agents, or, by exercising reasonable diligence, should have been known by Provider, its employees, subcontractors or other agents;

3.9.2. provide DOHMH with physical access to the affected locations and operations;

3.9.3. provide DOHMH with access to Provider employees, subcontractors and other individuals with knowledge of the Security Incident;

3.9.4. fully cooperate with and assist DOHMH in investigating the occurrence, including, without limitation, by providing full access to information necessary to determine the scope of the Security Incident such as all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by DOHMH;

3.9.5. immediately remedy the Security Incident at Provider's expense in accordance with applicable privacy rights, laws, regulations, policies, standards, and industry best practices;

3.9.6. allow DOHMH to participate in the root cause analysis, or Provider shall provide to DOHMH a detailed written root cause analysis for any breach or compromise;

3.9.7. provide DOHMH with updates when requested by DOHMH;

3.9.8. 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 private information, as defined in Section 10-501 or its successor of the Administrative Code of the City of New York ("**Private Information**"), at DOHMH's request and pursuant to DOHMH'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;

3.9.9. in the case of PHI/e-PHI or Private Information, 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;

3.9.10. be responsible for recovering and/or recreating lost DOHMH Data in the manner and on the schedule approved by DOHMH without charge to DOHMH;

3.9.11. bear the responsibility and all related costs for any Security Incident to the extent that DOHMH (or its employees, subcontractors or affiliates) is not at fault, 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. provide DOHMH with documentation that Provider's incident response plan has been implemented; and

3.9.13. provide DOHMH with a detailed corrective action plan describing the measures Provider shall undertake to prevent future occurrences as expeditiously as possible under the circumstances.

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, DOHMH 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 DOHMH 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 DOHMH.

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

IV. DATA PRIVACY AND INFORMATION SECURITY PROGRAM

4.1. Provider Privacy and Security Program. Without limiting Provider's obligation of confidentiality, as further described in this 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 DOHMH Data; (b) protect against any anticipated threats or hazards to the security, confidentiality, availability, or integrity of DOHMH Data; (c) protect against unauthorized or illegal or accidental disclosure, access to, destruction, alteration, modification, loss, acquisition or use of DOHMH Data; (d) ensure the proper disposal of DOHMH Data, if requested by DOHMH 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 DOHMH, and in no case shall the safeguards of such Privacy and Security Program be less stringent than the safeguards used by DOHMH.

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 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. 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 DOHMH Data. Provider understands and acknowledges that DOHMH 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 DOHMH.

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 DOHMH:

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 DOHMH Data;

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

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; and

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 DOHMH Data.

4.5.3. Privacy and Security Audit by DOHMH. Without limiting any other audit rights of DOHMH, DOHMH 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. DOHMH reserves the right to also perform relevant tests to ensure Provider is compliant with required security policies and standards. Provider shall permit DOHMH to perform such audit, including an audit of the physical security of any of Provider's premises applicable to the Cloud Services provided to DOHMH and shall fully cooperate and furnish all requested materials in a timely manner. The review and audit may be conducted remotely or onsite by DOHMH or a DOHMH provider and at DOHMH's expense. DOHMH 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 DOHMH, Provider shall complete, within forty-five (45) calendar days of receipt, an audit questionnaire provided by DOHMH regarding Provider's Privacy and Security Program. Provider shall not be entitled to compensation from DOHMH 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. The audit rights of DOHMH set forth in this Agreement will apply to IOT Devices and new devices used by Provider to provide the Services.

4.5.5. Usage Audit. In the event of a usage audit by Provider, Provider may conduct such audit by itself at its own cost, or engage the services of an Auditor at Provider's own cost. Provider or Auditor shall be bound by confidentiality terms no less stringent than those set forth in this Agreement. In conducting an audit pursuant to this Section 4.5.4, Provider or Auditor may request DOHMH for an analysis of the software DOHMH is running and Provider or Auditor may make copies of any such software logs to the extent necessary to verify the DOHMH's compliance with this Agreement. Provider or Auditor shall not run any software on the DOHMH's systems, nor shall Provider or Auditor conduct the audit at any of the City's premises. Provider or Auditor shall provide sixty (60) calendar days' notice prior to an audit. Any audit shall be performed during DOHMH's normal business hours and in a manner that minimizes disruption to its business.

4.5.6. Findings. Provider shall provide DOHMH 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 DOHMH with documentation of the remedial efforts within ten (10) days after their completion.

4.5.7. 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.

4.5.8. IOT Devices. Provider represents and warrants the IOT Device is NEMA certified and has a rating of 45 or better. During DOHMH's security review process (or earlier), Provider will provide DOHMH with the applicable NEMA rating and datasheet for the IOT Device. Provider will provide a five (5) year warranty, which (a) starts from the later of the date of purchase or the date of installation, and (b) includes replacement if the IOT Device is damaged within the warranty period. Provider will ensure that the IOT Device includes all hardware required to securely mount the IOT Device, including but not limited to appropriate locking mechanisms.

4.5.9. If Provider provides any other customer with an automated remote update mechanism, Provider will provide DOHMH with the automated remote update mechanism (that will allow for updates of all of the same IOT Devices) at no additional 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 DOHMH, Provider shall provide the audit logs to DOHMH 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 DOHMH, Provider shall also provide DOHMH with information about whether it patched critical vulnerabilities and the remediation steps it took.

4.8. Vulnerability Reporting and Notification Requirement. Provider shall inform DOHMH and NYC3 of any identified vulnerabilities in information systems no later than ten (10) business days after receiving notification. Provider shall provide a report to DOHMH and NYC3 that includes a detailed description of the identified vulnerabilities and a remedial plan with associated timelines informing DOHMH and NYC3 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; and

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 DOHMH of any enhancement, upgrade, or other change in the Cloud Service that may impact the security, availability, or performance of the Cloud Services.

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

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 DOHMH. 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, DOHMH'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.

VI. ENCRYPTION AND AUTHENTICATION

6.1. Provider shall encrypt all DOHMH Data, including backups, while at rest and in transit from end to end using encryption standards and methods that are approved and recommended by NIST and, is 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 City of New York / Head of Cyber Command. Proven algorithms such as AES-128, AES-

256, ECDH, Blowfish, PGP, RSA, WAP2 or WPA3 for Wi-Fi encryption and SSH v 2 for remote login must be used as the basis for encryption technologies. At a minimum, the hash algorithm must be 256bit SHA-2 and symmetric key encryption algorithm is AES-128. SSL/TLS implementations must use, at a minimum, version number 1.2 with cipher suite implementing Cipher Block Chain (CBC) or Galois/Counter modes (GCM) as modes of operation for the cipher component and 256bit SHA-2 for the digest component. A minimum of 2048 bit RSA key modulus must be used for key establishment and digital signatures. A minimum of P-256 curve must be used for elliptical curve key establishment and digital signatures.

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 DOHMH.

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. OTI is responsible for managing and operating Citywide CITYNET Certificate Authority. For internal City of New York namespaces OTI must generate digital certificates through the Citywide Certificate Authority (internal PKI), whereas for external namespaces trusted third party providers must be used.

VII. DOHMH 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 DOHMH. If such a security review has been completed and DOHMH’s written disposition requires Provider to comply with DOHMH’s prescribed security measures (“**DOHMH Security Measures**”), then, in addition to complying with this Agreement, Provider shall comply with DOHMH Security Measures.

7.2. Any written disposition of a security review by DOHMH shall not be deemed to constitute an endorsement of the Cloud Services or a certification that the Cloud Services meet DOHMH Security Measures or the requirements under this Agreement. Provider remains fully responsible for ensuring compliance with DOHMH Security Measures and this Agreement. At all times during the term of the Cloud Services, Provider agrees to cooperate with DOHMH to ensure that Provider is in compliance with all DOHMH 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 NYC3, submit information into the SSA tool, and (b) submit all devices, applications, systems, software and infrastructure used to support DOHMH systems to DOHMH’s applicable security testing process. DOHMH’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 DOHMH'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 DOHMH.

VIII. DATA OWNERSHIP

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

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

8.3. DOHMH 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 DOHMH. Any feedback from DOHMH is provided "as is", and DOHMH 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 DOHMH Data, any confidential information or Intellectual Property of DOHMH is conveyed to Provider.

IX. 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 DOHMH's use of the Cloud Services are not applicable to DOHMH, 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 DOHMH, including any other privacy policies of Provider and third party providers.

9.2. To be valid, any amendment to this Agreement must be in writing and signed by the Parties.

X. SEPARATION ASSISTANCE

10.1. In the event of impending or actual separation (due to impending or actual expiration or earlier termination of this Agreement whenever that may occur) and for up to ninety (90) days following such expiration or termination, DOHMH may request in writing that Provider do or permit DOHMH to do any of the following, or any combination of the following:

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

10.1.2. Destroy any DOHMH Data. Any written request by DOHMH directing Provider to destroy DOHMH Data shall specify what data DOHMH is requesting to be destroyed. Except for actions required by this Agreement, Provider shall not destroy any DOHMH Data in the absence of a specific written request from DOHMH. If Provider destroys any DOHMH Data, it shall verify such destruction in writing. Destruction of DOHMH 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 DOHMH, a request to destroy DOHMH Data includes destruction of live/production data as well as data housed as/in backup(s).

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

10.2. At no cost to DOHMH, Provider must provide separation assistance to DOHMH to perform or support the exporting, copying, and/or destruction of DOHMH Data in accordance with DOHMH's written request.

10.3. Additionally, in the event of a termination by DOHMH due to a breach by Provider of this Agreement, Provider shall provide transition assistance at no cost to DOHMH.

10.4. In the event the parties are negotiating a renewal contract, Provider will not withhold the Cloud Services due to a lapse in the subscription term and the ninety (90) day provision in Section 8.2 of this Agreement shall not apply during the negotiations. Provider shall continue to retain DOHMH Data unless otherwise instructed by DOHMH.

XI. CONFIDENTIALITY

11.1. Provider agrees to hold confidential, both during and after the completion or termination of this Agreement, all DOHMH Data. Provider shall use DOHMH Data for no purpose other than providing the Cloud Services in accordance with this Agreement.

11.2. Provider agrees to maintain the confidentiality of DOHMH Data by using a reasonable degree of care, and at least the same degree of care that Provider uses to preserve the confidentiality of its own confidential information.

11.3. Provider agrees that DOHMH Data shall not be made available to any person or entity without the prior written approval of DOHMH, except that Provider may disclose DOHMH Data to its employees, officers, agents and consultants ("**Representatives**") on a need to know basis to provide the Cloud Services to DOHMH. Provider shall ensure that its Representatives are bound by confidentiality obligations no less stringent than those in this Agreement, and shall be liable for a breach by its Representatives of the foregoing confidentiality obligations.

11.4. Provider shall not disclose DOHMH Data, or any information it receives pursuant to this Agreement, that is Personal Identifying Information (as defined in Section 10-501 of the New York City Administrative Code or successor) or Identifying Information (as defined in Section 23-1201 or successor), or information, which combined with publicly-available information, may reasonably be used to identify an individual.

11.5.The obligation under this section not to disclose shall not apply where Provider is legally required to disclose such reports, information or data, by virtue of a subpoena, court order or otherwise ("**disclosure demand**"), provided that Provider complies with the following unless prohibited by law: (a) Provider shall provide advance notice to DOHMH, in writing or by e-mail, that it received a disclosure demand for to disclose such reports, information or data, (b) if requested by DOHMH, Provider shall not disclose DOHMH Data until DOHMH has exhausted its legal rights, if any, to prevent disclosure of all or a portion of such Data, and (c) Provider shall reasonably cooperate with DOHMH in minimizing the DOHMH Data disclosed.

XII. ORDERS AND PAYMENT

12.1. Expenditures. Expenditures under this Agreement shall be determined by available funding levels. There is no guarantee of any expenditure level under this Agreement and DOHMH shall procure only the specific Cloud Services that it requires.

12.2. PPB Rules Applicability. All payment terms, fees and taxes are subject to the PPB Rules. In the event of a conflict between this Agreement and the PPB Rules, the PPB Rules shall take precedence.

XIII.RECORDS AND AUDIT

13.1 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.

13.2 Audit by DOHMH. 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**"), DOHMH, and the DOHMH's Office of the Inspector General, (b) the State, (c) the federal government, and (d) other persons duly authorized by DOHMH. Provider shall submit any and all documentation and justification in support of expenditures or fees under this Agreement as may be required by DOHMH and by the Comptroller in the exercise of his or her powers under law.

XIV. ADDITIONAL SECURITY REQUIREMENTS

14.1. Citywide Information Security Policy. Provider shall comply with the Policies and Standards. In addition, Provider shall ensure that all subcontractor(s) approved by DOHMH in writing (each an "**Authorized Subcontractor**") and any employee of Provider or an Authorized Subcontractor who needs to know DOHMH Data in order to perform Provider's obligations (each an "**Authorized Person**") who may have access to any DOHMH Data or DOHMH Information 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.

14.2. OTI User Responsibility Policy ("**URP**"). Provider shall require each Authorized Person who may have access to any DOHMH Information 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 DOHMH project manager, or a person designated by DOHMH, within fifteen days (15) days after the Authorized Person is assigned to perform Services pursuant to this Agreement.

14.3. Non-Disclosure Agreement. If requested by DOHMH, 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 DOHMH Data to execute a Non-Disclosure Agreement in a form acceptable to DOHMH.

14.4. Cooperation with Accreditation. Provider shall cooperate with and facilitate the successful completion of any security accreditation tasks and processes relevant to the Cloud Services it provides. Provider shall complete said security accreditation tasks and processes within thirty (30) business days unless granted an extension by DOHMH.

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

14.6. Noncompliance Self Reporting Requirement. Provider shall notify DOHMH and NYC3 of any changes to the infrastructure of all information systems that would affect DOHMH 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 DOHMH and NYC3 no later than three (3) business days after the change has occurred. For noncompliance, Provider shall submit to NYC3 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.

14.7. Remote Access Methods. Provider must obtain written permission from DOHMH for each instance of remote access it wishes to use and access DOHMH Information Assets.

XV. TERM AND TERMINATION

15. Term. This Agreement shall commence on the Effective Date and shall expire at the time that DOHMH no longer has a license to use the Cloud Services, unless terminated earlier pursuant to this Section XV.

DOHMH may terminate this Agreement as follows:

15.1. Termination for Cause. Immediately, if Provider commits any material breach of this Agreement and fails to cure such breach within thirty (30) days after DOHMH notifies Provider in writing of such breach; or

15.2. Termination for Convenience. With or without cause by giving Provider fifteen (15) days prior written notice of termination.

15.3. Termination Consequences.

15.4. In the event of a termination for cause under Section 15.1 or a termination for Security

Incident under Section 3.1, all fees for Cloud Services provided after the date of the breach will be deemed to be waived by Provider, and Provider shall within the following thirty (30) days refund any waived fees that have been paid. This provision is in addition to any rights that DOHMH may have to recover damages under this Agreement or pursuant to applicable law.

15.5. In the event of a termination for convenience under Section 15.2, DOHMH shall, upon termination, pay to Provider the total undisputed amounts due and which accrued under this Agreement as of the termination date.

XVI. GENERAL

16.1. Order of Precedence. This Agreement takes precedence over any provision in any other separate agreement between DOHMH and Provider, and DOHMH and Reseller. In the event of a conflict between this Agreement and any other separate agreement, this Agreement shall prevail.

16.2. Survival. All terms of this Agreement that should by their nature survive termination shall survive, including, Section III (Data Management and Security), Section IV (Data Privacy and Information Security Program), Section 16.3 (Limitation of Liability), Section 16.4.2 (Intellectual Property), Section 16.5 (Publicity), Section 16.6 (Indemnification), and Section 16.8 (Source Code Escrow).

16.3. Limitation of Liability

16.3.1. Subject to the provisions of Section 16.3.2 below, each Party's aggregate liability for all claims arising out of the Cloud Services, whether in contract, tort or otherwise, shall not exceed the greater of: (a) forty-eight (48) times the average monthly charges paid by DOHMH to Provider (or Reseller, if any), calculated over the prior twelve (12) month period immediately preceding the date on which liability for the claim first arose; (b) three times (3x) the contract value; or (c) one million dollars ($1,000,000).

16.3.2. The limitation of liability set forth in Section 16.3.1 above shall not apply to Provider's liability arising out of any of the following: (a) Provider's indemnification obligations under this Agreement; (b) Provider's breach of the confidentiality provisions in this Agreement; (c) Provider's breach of Section III (Data Management and Security) or Section IV (Data Privacy and Information Security Program) of this Agreement, (d) the infringement by Provider, or any of its Affiliates or subcontractors, of the Intellectual Property of DOHMH or of a third party; and (e) to the extent prohibited by law.

16.3.3. To the extent that Provider may be liable to the City (which includes DOHMH) for any action, inaction or operation of Provider under this Agreement, or under statutory or common law, for which a Reseller may also be liable, Provider's and the Reseller's (if any) liabilities are joint and several, and DOHMH is not limited in its ability to seek recourse from one or the other.

16.3.4. The City (which includes DOHMH) shall not be liable to Provider for indirect, incidental, consequential, exemplary, reliance, special or similar damages, including damages for lost profits, regardless of the form of action, with regard to or arising out of the use or provision of the Cloud Services or any other conduct under this Agreement.

16.3.5. Any provision in the any other agreement limiting or disclaiming Provider's liability is hereby deemed to be void and unenforceable.

16.4. Warranties and Representations.

16.4.1. Uptime and Service Credits. Provider represents and warrants that the Cloud Service shall function in accordance with the service level agreement ("**SLA**") annexed hereto as Attachment A. In the event Provider fails to meet agreed-upon service levels in Attachment A, Provider shall provide the City (which includes DOHMH) with service credits pursuant to Attachment A.

16.4.2. Intellectual Property. Provider represents and warrants that it has the rights necessary to provide the Cloud Services to the City (which includes DOHMH) in accordance with this Agreement.

16.4.3. 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 Agreement and consistent with Provider's best practices; (b) Provider shall provide adequate training, as needed, to DOHMH 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 does 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; (f) there is no pending or threatened litigation involving Provider that may impair or interfere with the City's (which includes DOHMH's) right to use the services; and (g) Provider has sufficient authority to enter into this Agreement and grant the rights provided in such Agreement to the City (which includes DOHMH).

16.5. Publicity. Provider shall notify DOHMH, at any time either during or after completion or termination of this Agreement, of any intended statement to the press or any intended issuing of any material for publication in any media of communication (print, news, television, radio, Internet, etc.) regarding the services provided or the data collected pursuant to this Agreement at least 24 hours prior to any statement to the press or at least five business days prior to the submission of the material for publication, or such shorter periods as are reasonable under the circumstances. Provider may not issue any statement or submit any material for publication that includes DOHMH Data. Provider shall not use the City's or DOHMH's name and trademarks without DOHMH's prior written consent.

16.6. Indemnification

16.6.1. 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.

16.6.2. 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.

16.6.3. No Indemnification by the City. Any provision in any separate agreement requiring the City (which includes DOHMH) to provide indemnification is hereby deemed to be void and unenforceable.

16.7. Use of Third Party Providers

16.7.1. Provider must identify any third party entities involved in the provision of the Cloud Service and provide DOHMH with a copy of Provider's agreement with the third-party provider. The agreement must be approved in writing by DOHMH. Provider shall notify DOHMH 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 DOHMH'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 DOHMH; 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 DOHMH 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.

16.7.2. 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 DOHMH. 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 Agreement to the contrary is deemed to conflict with this Agreement.

16.8. Source Code Escrow. The Parties agree that in the event Provider becomes: (a) insolvent or bankrupt, (b) makes an assignment for the benefit of creditors, or (c) voluntarily or involuntarily initiates bankruptcy, insolvency, or reorganization proceedings, then DOHMH and Provider shall negotiate in good faith to enter into a source code escrow agreement with a mutually agreed-upon source code escrow company setting forth source code escrow deposit procedures and source code release procedures, which include testing and review of such escrow.

16.9. Governing Law; Jurisdiction and Venue; Jury Waiver; No Arbitration. The laws of the State of New York, without reference to its choice of law principles, govern this Agreement, and any claims arising out of or relating to this Agreement, or their negotiation, execution, performance, or breach. All disputes and controversies arising out of or relating to the negotiation, execution, performance or breach of this Agreement must be resolved in accordance with the PPB Rules and in the New York State or federal courts in the City, County and State of New York, and each party irrevocably consents to the exclusive venue and personal jurisdiction of those courts for the resolution of disputes and waives all objections thereto. To the fullest extent permitted by law, each party irrevocably waives its right to a jury in any litigation arising out of or relating to this Agreement, their negotiation, execution, performance or breach. No dispute, controversy or claim arising out of or relating to this Agreement or the enforcement, breach, termination or validity thereof shall be submitted to arbitration or similar dispute resolution method.

16.10. Fees.

16.10.1. DOHMH is not responsible for an early termination fee.

16.10.2. Upon any termination of a Cloud Service, Provider shall within the following thirty (30) days promptly refund all unused prepaid fees.

16.10.3. Rates and fees may only be increased pursuant to a written amendment to this Agreement that has been signed by both parties. Overage and excess usage fees are not permitted in the absence of DOHMH's prior written agreement.

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

16.10.5. DOHMH's payment of an invoice without objection or failure to raise an objection to an invoice shall not constitute a waiver of any objections to that invoice.

16.11. Insurance

16.11.1. 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 $10,000,000 per claim and $20,000,000 in the aggregate. This policy must include coverage for:

16.11.1.1. failure to protect confidential information, including identifying information;

16.11.1.2. failure of the security of Provider's computer systems;

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

16.11.1.4. 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;

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

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

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

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

16.11.1.9. 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;

16.11.1.10. Media liability; and

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

16.11.2. <u>Technology Errors and Omissions</u>. 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 $10,000,000 per occurrence and $20,000,000 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.

16.11.3. <u>General Insurance Requirements</u>

16.11.3.1. All required insurance policies must be maintained with companies that may lawfully issue the policy and have an A.M. Best rating of at least A- / "VII" or a Standard and Poor's rating of at least A, unless prior written approval is obtained from the City Law Department.

16.11.3.2. All insurance policies shall be primary (and non-contributing) to any insurance or self-insurance maintained by the City.

16.11.3.3. All insurance policies shall cover the City, together with its respective officials and employees, as additional insured.

16.11.3.4. The City's limits of coverage for all types of insurance required under this Article shall be the greater of (a) the minimum limits required in this Agreement, or (b) the limits provided to Provider as named insured under all primary, excess, and umbrella policies of that type of coverage.

16.11.3.5. Policies of insurance provided pursuant to this Agreement must be primary and non-contributing to any insurance or self-insurance maintained by the City.

16.11.3.6. If Provider receives notice from an insurance company or other person that any insurance policy required under this Agreement shall expire or be cancelled or terminated for any reason, Provider shall immediately forward a copy of such notice to DOHMH, and the New York City Comptroller, Attn: Office of Contract Administration, Municipal Building, One Centre Street, Room 1005, New York, New York 10007.

16.11.3.7. Insurance coverage in the minimum amounts required in this Article shall not relieve Provider or its subcontractors of any liability, nor shall it preclude the City from exercising any rights or taking such other actions as are available to it.

16.11.3.8. Provider waives all rights against the City, including its officials and employees, for any damages or losses that are covered under any insurance required under this Agreement (whether or not such insurance is actually procured or claims are paid thereunder) or any other insurance applicable to the operations of Provider or its subcontractors in the performance of Cloud Services.

16.11.3.9. All claims-made policies must have an extended reporting period option or automatic coverage of not less than two (2) years. If available as an option, Provider shall purchase extended reporting period coverage effective on cancellation or termination of the claims-made insurance unless a new policy is secured with the same retroactive date as the expired policy.

16.12. Open Source Software. If the Cloud Services consist of any Open Source Software, Provider shall, upon request, furnish DOHMH 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 DOHMH in advance of its processing of any order for such Cloud Services.

16.13. Assignment. Provider may not assign or delegate its rights and/or obligations, or any part thereof under this Agreement to any or all of its Affiliates without DOHMH's prior written consent. Any attempted assignment or transfer by Provider of this Agreement is null and void.

16.14. Severability. All rights and remedies whether conferred in this Agreement, 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. The terms and conditions stated herein are declared to be severable. If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

16.16 Notices. Provider shall submit notices as required in this Agreement as follows:

To DOHMH:

New York City Department of Health and Mental Hygiene
42-09 28th Street
Long Island City, New York 11101
Attn: ________________________________

To DOHMH regarding Security Incidents: Philip Bores, pbores@health.nyc.gov, 347-396-2240, and Nicholas Elcock, nelcock@health.nyc.gov, 917.654.1279

To DOHMH regarding anything other than Security Incidents: ______________________________

To NYC3 regarding Security Incidents: soc@cyber.nyc.gov, vuln@cyber.nyc.gov and 718-403-6761

To NYC3 regarding anything other than Security Incidents: CISO@cyber.nyc.gov

[REMAINDER OF PAGE INTENTIONALLY BLANK – SIGNATURES FOLLOW]

IN WITNESS WHEREOF, and intending to be legally bound, the Parties hereto have executed this Agreement as of the Effective Date.

NEW YORK CITY DEPARTMENT OF HEALTH AND MENTAL HYGIENE	PROVIDER
By: ______________________________	By: ______________________________
Name: ___________________________	Name: ___________________________
Title: ____________________________	Title: ____________________________
Date: ____________________________	Date: ____________________________

ATTACHMENT A
SERVICE LEVEL AGREEMENT

1. INTRODUCTION

This attachment Service Level Agreement ("**SLA**") to the Agreement describes the performance standards and service levels to be achieved by Provider in providing the Cloud Services. This is subject to the provisions of the Agreement which are incorporated herein by reference. In the event of a conflict between the provisions of the Agreement and any provision of this SLA, the Agreement will govern.

2. DEFINITIONS

Unless otherwise set forth in this SLA, capitalized terms not separately defined will have the respective meanings ascribed in the Agreement. As used in this SLA, the following terms shall have the following meaning:

2.1 "**Available**" or "**Availability**" means the Cloud Services shall: (a) be available for access and use over the Internet; (b) provide the functionality and content required under the Agreement and any applicable work order; and (c) operate without any Severity 1 or Severity 2 Defect, other than a minor malfunction that does not impact an Authorized User's ability to use the Cloud Services to achieve an intended goal.

2.2 "**Days and Hours of Coverage**" means the days of coverage as set out in Section 4.1 of this SLA.

2.3 **"Defect"** means a malfunction of the Cloud Service resulting in functionality differing from expected functionality as designed or a failure of the Cloud Services to operate in accordance with its documentation, the Agreement and this SLA.

2.4 "**Force Majeure**" means an act or event beyond the control and without any fault or negligence of Provider. Such events may include, but are not limited to, fire, flood, earthquake, storm or other natural disaster, civil commotion, war, terrorism, riot, and labor disputes not brought about by any act or omission of the Provider.

2.5 **"Software Patch"** means a fix to one or more Defects.

2.6 **"Severity Level"** means the level assigned to a reported Defect by DOHMH based on the description of the Defect under this SLA.

2.7 "**Problem**" means an unknown underlying cause of one or more Defects.

2.8 "**Response Time**" means the response time linked to the relevant Severity Level as set forth in this SLA.

2.9 "**Resolution Time**" means the resolution time linked to the relevant Severity Level as set forth in this SLA.

2.10 "**Service Credits**" means the support services fees credited to DOHMH following claim approval as set forth in this SLA.

2.11 "**Severity 1**" means a Defect that ____________________________.

2.12 "**Severity 2**" means a Defect that ____________________________.

2.13 "**Severity 3**" means a Defect that ____________________________.

2.14 "**Severity 4**" means a Defect that ____________________________.

2.15 **"Subscription Fee"** means the amount paid by DOHMH to Provider for the procurement of the license/s to the Cloud Services.

2.16 "**Ticket**" means any registration in the Provider's helpdesk system for an identified Problem.

3. AVAILABILITY REQUIREMENT

3.1 Provider shall ensure that Cloud Services shall be Available 99.9% of the time, excluding the time the Cloud Services are not Available as a result of one or more of the exceptions in Section 3.2.

3.2 No period of Service downtime will be included in calculating Availability to the extent that such downtime is caused by any of the following:

3.2.1 Any planned downtime of which Provider gives at least one (1) week advance notice to DOHMH;
3.2.2 Any delay, act or omission by DOHMH, access to or use of the Cloud Services by DOHMH, or using DOHMH's user identification and password, that does not comply with this Agreement; or
3.2.3 A Force Majeure event.

3.3 For any partial calendar month during which DOHMH subscribes to the Cloud Services, Availability will be calculated based on the entire calendar month, not just the portion for which DOHMH subscribed. This includes when the system may be Available but there are outstanding Severity 1 and Severity 2 issues that are critical or significant business impact.

3.4 Should the Availability of Covered Services fall below the threshold set forth in Section 3.1 hereto in a calendar month, Provider shall provide a credit as set forth in the table below:

Availability	Service Credit
99.5% to 99.8%	one percent (1%) of monthly Subscription Fee
98% to < 99.5%	two percent (2%) of monthly Subscription Fee
95% to <98.0%	five percent (5%) of monthly Subscription Fee
< 95%	one hundred percent (100%) of the monthly Subscription Fee.

3.5 Any service credits duly claimed by DOHMH under Section 3.4 and Section 6.7 shall be promptly remitted to DOHMH either by direct payment, or withheld as a set-off against pending invoices submitted by Provider pursuant to a work order or this Agreement, at DOHMH's election.

4. SUPPORT

4.1 The Provider shall perform its support obligations during the following Days and Hours of Coverage:

4.1.1. Twenty-four (24) hours a day, seven (7) days a week for Severity 1 and 2 Defects; and
4.1.2. Business Days, 8:00 AM to 12:00 AM EST for all other Severity Levels.

4.2. All support (including remote support) must be provided by Provider from the United States.

4.3. During the Days and Hours of Coverage, Provider shall provide the following support services:

4.3.1. Technical support, which shall include assisting DOHMH in its use of the Cloud Services, resolving technical Defects, and communicating relevant information regarding the Cloud Services;
4.3.2. Communication support, which shall include help desk support, unlimited telephone and email consultation and resolution communication support;
4.3.3. Administrative support, which shall include user maintenance (administrative provisioning, password resets), troubleshooting assistance and responses to general inquiries; and
4.3.4. Provision of documentation, which shall include incident reports and reports on Provider's compliance with Response Time and Resolution Time requirements under this SLA.

5. SUPPORT REQUESTS

5.1. Provider will grant access to a system where DOHMH can communicate potential Defects to the Provider.

5.2. If DOHMH encounters a problem Defect in the usage of the Cloud Services, DOHMH shall (a) diagnose and reasonably assign a Severity Level to the noted Defect; and (b) send a support request to Provider by opening a Ticket.

6. INCIDENT MANAGEMENT

6.1. Provider shall promptly conduct a root cause analysis of the Defect upon notification. If Provider discovers the Defect before DOHMH does, Provider shall diagnose and reasonably assign a Severity Level to the noted Defect. DOHMH may require that the Defect be assigned a different Severity Level. Provider may advise DOHMH and dispute DOHMH's determination.

6.2. The Provider shall investigate and rectify a Defect in accordance with the applicable Severity Levels, Response, and Resolution Times.

6.3. In the event a Defect is determined to be caused (in whole or in part) by the Cloud Services, the Provider will be liable for all failures to meet the Response and Resolution times listed in Section 6.4 which may then result in Service Credits.

6.4. Severity Level, Response and Resolution Times during Days and Hours of Coverage are defined in the following table:

Severity Level	Response Times	Resolution Times
Critical (1)		
Major (2)		
Medium (3)		
Minor (4)		

[1] 'Correction available' means that a Software Patch is ready to be implemented by DOHMH with support from the Provider.

[2] Note that Parties can mutually agree in writing to increase the Resolution Times inside Hours of Coverage.

6.5. The Response Time shall be calculated from the moment a Ticket is initiated until the moment a repair commences.

6.6. Resolution Time shall be calculated as the time between the initiation of the Ticket by DOHMH according to the mutually agreed upon procedures and the time the Provider's Service Desk declares the actions to resolve the Defect in the Ticket completed as verified by DOHMH.

6.7. If the Provider fails to provide the incident management services within the agreed timelines as set forth in 6.4, DOHMH is entitled to claim Service Credits as follows:

Severity Level	Qualification Period	Service Credit
(1) Critical	Each day or part of a day that the applicable response and resolution time in Section 6.6 has been missed.	$___ per day or partial day.
(2) Major	Each day or part of a day that the applicable response and resolution time in Section 6.6 has been	$__ per day or partial day.

	missed.	
(3) Medium	Each day or part of a day that the applicable response and resolution time in Section 6.6 has been missed.	$__ per day or partial day.
(4) Minor	N/A	N/A

6.8. Failure on the part of the Provider to provide a correction or a workaround for a Severity 1 or Severity 2 Defect within seven (7) consecutive days provides DOHMH with the option to engage a third-party to fix the issue, while preserving DOHMH's right to terminate in accordance with the Agreement.

Version	**Date**
1.0	March 2022
2.0	August 2023
2.1	July 2024