APPENDIX C

PRIVACY, SECURITY, AND RESILIENCE

This is an Appendix attached to and incorporated by reference with the Agreement made on October 1, 2019 between the CITY OF BERKELEY ("City") and <Vendor's Name>, ("Consultant"), providing for the licensing and services related to the <Vendor's Name> hosted software system (Software).

1. INFORMATION SECURITY AND PRIVACY

1.1. Consultant understands and agrees that, in the performance of the services under this Agreement, Consultant may have access to private or confidential information owned or controlled by City and that such information may contain confidential or proprietary details, the disclosure of which to third parties may be damaging to City.

1.2. Consultant's provision of Hosted Services requires Consultant to collect information that may include confidential and private information from/or about third parties.

1.2.1. Consultant is not authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as privacy data.

1.2.2. Consultant is authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as Health Insurance Portability and Accountability Act ("HIPAA") regulated data (including records and metadata). City, Consultant, and Consultant's third-parties (Party) have obligations to protect the privacy and provide for the security of protected health information disclosed to Consultant and their third-parties under this Contract pursuant to HIPAA, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and regulations promulgated thereunder including 45 CFR Sections 160 and 164. City and Consultant agree to comply with the Business Associate Addendum (BAA), attached as Exhibit C and made a part of this Contract.

1.2.3. Consultant is authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as privacy data but not Health Insurance Portability and Accountability Act ("HIPAA") regulated data (including records and metadata). Vendor shall retain data only for deliberate, documented purposes. Vendor shall ensure that the longest retention period any privacy data is subject to dictates the end of that data's business purpose defined by City and this Agreement

1.3. Consultant will store the information on a secure remote server using reasonable safeguards in accordance with the Security Standards of the Agreement codified in DATA SECURITY (Section 2 below) and Consultant's published on-line privacy policies and in compliance with applicable laws, codes of practice, and other legal obligations associated with the collection, use, and disclosure of personal information. Consultant shall exercise

the same standard of care to protect such information as a reasonably prudent Consultant would use to protect its own proprietary and confidential data. City will be responsible for protecting the privacy and security of any information that City retrieves from Consultant's servers and shall prevent any unauthorized or illegal use or dissemination of such information and shall be solely responsible for ensuring compliance with any applicable data and privacy protection laws, codes of practice, and other legal obligations associated with the collection, use and disclosure of personal information by City, including such disclosure to Consultant as is necessary for Consultant to provide the Services to City. City shall exclusively own the personal data collected and managed by Consultant in connection with the Hosted Services, provided however that Consultant is granted a royalty-free, perpetual, non-exclusive right and license to use, reproduce, distribute and adapt the collected data as is necessary for Consultant to perform its obligations under this Agreement.

1.4. Compliance with laws: CONSULTANT shall comply with any statutes and regulations that apply to its provision of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to the privacy and security of personal information, including trans-border data transfers and data breach notification requirements as required of CONSULTANT by law. City of Berkeley shall comply with all laws that apply to its use of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to collection and processing of City Data in CONSULTANT systems through the Subscription Service. City agrees to provide any required disclosures to and obtain any required consents for the transfer of City Data to CONSULTANT.

2. DATA SECURITY

Consultant shall establish, implement and maintain security written procedures, practices and internal controls appropriate to information technology (IT) service Consultants (ITSP) to support the following minimum information security standards (these "Security Standards") which protect City Data from unauthorized access, destruction, use, modification, or disclosure, as described in Consultant's Data Security Guide attached hereto, and incorporated herein by reference:

2.1. ADMINISTRATIVE CONTROLS

2.1.1. Security Officer: Appoint a head security officer to be responsible for implementing policies, procedures and internal controls to carry out these Security Standards.

2.1.2. Cyber-Resilience Program: Document in a Data Security Guide the Consultant's cyber-resilience program. Consultant's cyber-resilience program will include, at a minimum: (i) physical, administrative and technical security controls; (ii) service interruption and data breach notification procedures (such as runbook) and metrics; (iii) release and system upgrade policy and procedures that include and address cybersecurity; (iv) service and disaster availability procedures (such as runbook) and metrics; and (v)

Consultant's security, governance, and compliance policy and procedures applicable to its third-parties.

2.1.3. Personnel Security: To the fullest extent allowed under applicable laws, Vendor shall not hire, retain or engage officers or employees (including de facto employees, or agents or third-party contractors having officers or employees), collectively "Workers," who have been convicted of or entered into a court-supervised diversion program for fraud, embezzlement, larceny, perjury, terrorism, or breach of trust or fiduciary duty, to perform any responsibilities or functions in connection with:

- Processing City's private or confidential information owned or controlled by City, or
- Creating, programming, or maintaining security-related IT environments, systems, applications, or technical services in connection with the Agreement

2.1.4. Personnel Training: Train Workers on these Security Standards, and contractually bind Workers to the obligation to comply with these Security Standards and maintain the physical, operational and technological security of City private and confidential information.

2.1.5. Secure Areas: Restrict, control and monitor all physical and logical areas in Consultant's IT environments that contain City private and confidential information, servers, switches, developers and administrators' work areas, or other operationally sensitive equipment ("Secure Area"). Physical Secure Areas controls are addressed are addressed in Physical Controls (Section 2.4). Logical Secure Areas controls are addressed in Technical Controls (Section 2.5) and Remote Access (APPENDIX D).

2.1.6. Approved Access: Approve all physical and logical access for physical and logical Secure Areas. Consultant's Secure Area access-approval process must be documented and records must be maintained for three (3) years.

2.2. TESTING

2.2.1. Disaster Recovery (DR) Testing: Test Consultant's DR plan each time the plan is re-published, but not less than once every twelve (12) months, by using any of several standard testing methods, including without limitation structured read-throughs, scenario or tabletop testing, functional testing, and full-scale testing.

2.2.2. Security Testing: Implement a repeatable and documented set of security tests for hardware, software and services – including but not limited to the production environment, releases of Software-as-a-Service (SaaS), other Cloud-based "as-a-Services" (PaaS, IaaS, DRaaS, etc.), containers and application program interfaces (APIs) used to deliver services of the Agreement or host City data within the scope of the Agreement. Determine the objectives of each security test, and tailor the approach accordingly. Analyze findings, and develop mitigation techniques to address (i) poor testing effectiveness metrics and (ii) any weaknesses discovered

through the tests. At the City's request, cooperate with City and its contracted resources to conduct security quality assurance and penetration tests on a mutually agreeable schedule.

2.3. RECORD RETENTION.

2.3.1. IT Operations Logs and Records: Maintain, and be prepared to show City at City's request, complete, clear and accurate logs, trouble-ticket logs, records of patches applied, and reports documenting the security tools, devices, measures, controls, procedures and practices for implementing these Security Standards.

2.3.2. Logical Access Logs and Records: Retain all identity and access management (IAM) records for at least three years, and make them available for City's inspection in accordance with the audit provisions of the Agreement. Records need not be retained on systems brokering access. At minimum, the identity and date and time of access by any party (including but not limited to Workers) as well as all changes in elevated privileges must be included. Include in these records signed approvals, following Consultant's Secure Area access-approval process, for access to and the hierarchy of provisioned privileges within logical Secure Areas by Workers and any other persons authorized.

2.3.3. Physical Access Logs and Records: Retain for at least three years all physical access records for all Secure Areas that host or access IT used to deliver hardware, software and services – including but not limited to releases of Software-as-a-Service (SaaS), other Cloud-based "as-a-Services" (PaaS, IaaS, DRaaS, etc.), containers and APIs to City under the Agreement, and make them available for City's inspection in accordance with the audit provisions of the Agreement. At minimum, the identity and date and time of access by any party (including but not limited to Workers) must be included. Include in these records signed approvals, following Consultant's Secure Area access-approval process, for access to physical Secure Areas by Workers and any other persons authorized

2.3.4. Incident Logs: Provide City with a quarterly consolidated report that includes all reported and researched security incidents.

2.3.5. DR Test Results: Report in writing the results of each DR test and deliver the written test results, certified and signed by Consultant's authorized officer, to City's Department of IT within ninety (90) days following completion of the test. The report must include: (i) any errors, omissions, inaccuracies and outdated information discovered in the DR plan by the test, (ii) corrective action planned for these errors, omissions, inaccuracies and outdated information, and (iii) the date by which Consultant will complete corrective actions.

2.4. PHYSICAL CONTROLS

2.4.1. PHYSICAL ACCESS MANAGEMENT

Implement and regularly test the following physical security measures in each physical Secure Area, as detailed below:

2.4.1.1. Card Access Control: Use card-access controls to partition physical Secure Areas.

2.4.1.2. CCTV coverage: Use CCTV monitoring and recording devices, including motion-activated devices, in all physical Secure Areas containing: hard copies of City private and confidential information, including without limitation our proprietary operational information); servers, transfer switches, telecomm link-lines or card-access system links; access areas to and from general work areas; hardware security modules (HSM) and key management equipment, tokens and codes; and all sensitive/restricted areas.

2.4.1.3. Physical security presence: Use guards where Card Access Control and CCTV coverage are not possible or are not industry best practice.

2.4.1.4. Security management monitoring: Use supervisors, staff monitoring CCTV, and other overseers of physical security to ensure dual-control of physical Secure Areas.

2.4.1.5. Segregate all City's physical and virtual IT environments, servers, switches and operationally sensitive instances and equipment from those for services and functions Consultant performs for Consultant's clients and consumers other than City.

2.4.1.6. Do not allow Consultant's outside support-services personnel to access physical Secure Areas. All access to these areas by support services personnel must be controlled, documented and physically accompanied by Consultant's pre-approved staff.

2.5. TECHNICAL CONTROLS

2.5.1. SYSTEMS AND APPLICATIONS RESILIENCE.

2.5.1.1. Consistent Emphasis on Security: Throughout the design, development and distribution (in any medium) of IT environments, service, containers, systems, releases, hardware and software applications and APIs, consistently apply information-security and technology-security considerations, and maintain industry-relevant, state-of-the-art security tools, devices, measures, controls, procedures and practices.

2.5.1.2. Fully Documented Features: Develop hardware, software and services – including but not limited to releases of Software-as-a-Service (SaaS), other Cloud-based "as-a-Services" (PaaS, IaaS, DRaaS, etc.), containers and APIs – by using only fully documented features that do not disregard or circumvent these Security Standards, including without limitation, bypassing or blocking security controls. Promptly report to City (during the design phase) any deviations from the foregoing requirement and cooperate with and support City to remove those deviations. If Consultant or City discovers any inadequate or inappropriate security, promptly take corrective action. Cooperate with City if same decides to block or remove/de-install Consultant's product from City IT

until the undocumented features and/or security-threatening deviations are corrected. Ensure that hardware and software developed by agents and third-party contractors also meet these requirements.

2.5.1.3. Change and Version Management: Maintain configurations and versions of products or services (including without limitation releases, software, containers, and APIs) through change management and version control. Maintain hard-copy and electronic documents showing the configuration and version control of products and services that Consultant delivers to City under the Agreement. Normally, a Change Control Request (CCR) shall be submitted by Consultant as a notification to the City Change Advisory Board (CAB) – no approval is required. When City testing of the CCR is anticipated or required, Consultant shall submit CCR at least two (2) weeks advanced and CCR must be approved by CAB. CCRs disapproved by CAB cannot be implemented by Consultant.

2.5.1.4. Data Back-up: Protect and back-up releases, software containers and APIs, program files and data, and all City's data, including without limitation City's private and confidential information needed for the operation of Agreement-required functions to a secure off-site location (sufficiently distant so as to avoid the effects of an interruption that affects your processing center).

2.5.1.5. Continuity: In the event the hosted service or any component thereof is rendered inoperative as a result of a natural or other disaster, continue to meet the terms and requirements of the Agreement through alternative means until your Agreement-required functions are recovered.

2.5.1.6. Restoration: In the event the hosted service or any component thereof is rendered inoperative as a result of a natural or other disaster, complete the recovery, resumption, and/or restoration activities as described in Consultant's DR Plan to achieve the Recovery Time Objective (RTO) of each affected function.

2.5.1.7. Unrecoverable Disaster: In the event the hosted service or any component thereof is rendered permanently inoperative as a result of a natural or other disaster, Consultant will make all commercially reasonable efforts to facilitate the expeditious restoration of the services. Where Consultant is unable to restore Services in a reasonable timeframe as specified by service-level agreement (SLA), City may exercise its right to terminate the agreement.

2.5.2. LOGICAL ACCESS MANAGEMENT.

Consultant's identity and access management (IAM) technology implements:

2.5.2.1. Least Privilege: Limits systems access to Workers and resources that are needed to perform specific responsibilities or functions.

2.5.2.2. Access Accounts: Assigns an individual account to each Worker who is given systems access. The access account must be authorized through NEXGEN' documented IAM system and registered to the individual Worker.

2.5.2.3. Authentication and Authorization Credentials: Requires each access-authorized Worker to use an authentication mechanism and unique credentials (e.g., ID and passcode/password) for that Worker's access account. Prohibits Workers from writing down, from sharing such credentials with anyone, from storing such credential in login scripts or other human-readable forms, from hard-coding such credentials in computers, from placing such credentials in any other locations, or from programming such credentials into function keys without appropriate login controls and encryption protection. Powerful accounts must be afforded strong protection, such as multifactor authentication (MFA/2FA) for administrators.

2.5.2.4. Process and Service Accounts: Assigns process and service accounts. Define and classify process and service accounts. Proactively manage, monitor, and control process and service account access by automatically discovering and storing accounts; scheduling credential rotation; audit, analyze, and manage activity; and monitor credentials to quickly detect and respond to suspicious and malicious activity.

2.5.2.5. Worker Access Review and Termination: Periodic access reviews that audit and monitor all users, especially those with elevated rights, on the Consultant's systems, and enable the immediate termination of access and privileges as warranted by change of job duties or termination in accordance with the principle of least privilege. The access of City Workers for whom we have given written notice to Consultant must be blocked or the authentication mechanism must otherwise invalidate access attempts within one (1) day of notice. Documentation of access reviews and termination actions must facilitate reporting to and examination by the City.

2.5.2.6. **Cloud Access Provisioning:** Cloud Service Consultants (CSP) support City's use of a Cloud Access Security Broker (CASB), including but not limited to managing an Internet Protocol (IP) whitelist and IPSEC/GRE tunneling, as appropriate, to explicitly restrict and permit traffic into and out of City's instance.

2.5.3. UNAUTHORIZED TRAFFIC

Design, develop and maintain instances, releases, devices, networks and systems (collectively, "IT") and the connectivity of Consultant's IT to City IT (or to the IT of the City's third-party contractors) which prevent unauthorized traffic from accessing or passing through City IT (or the IT of the City's third-party contractors).

2.5.3.1. Storage, Handling and Disposal of City Data: Separate and segregate all City private and confidential information received (whether received from the City or from another source), developed or processed under the Agreement from all information other than City data. At a minimum, encrypt all such data in storage and transit following industry standards and as technology permits. Where specified by the City, provide the City the capability to encrypt private and confidential information using City owned and managed key management technologies. Unless The City directs otherwise, properly destroy City private and confidential information when no longer required by the business processes of the Agreement, in accordance with industry best practices, provided that such destruction meets any requirements that the City reasonably specifies.

2.5.3.2. Security Vulnerability Notification and Resolution: Subscribe to third-party, industry-recognized security-vulnerability and security-notification services applicable to Consultant's IT used to store, handle or dispose of City private and confidential data. In a timely manner, review associated notifications and patches, test patches, schedule and apply patches, validate patch implementation, and record the findings, results and action taken (scheduled and ad hoc) as a result of these reviews. Include, at a minimum, security vulnerability resolution measures within Consultant's release cycle cadence.

2.5.3.3. Security Health Check and Certification: Make viewable to the City any applicable third-party security health/hygiene services and vulnerability/security scoring services to which the Consultant subscribes. At a minimum, make viewable to the City (electronically or as a report) all third-party certifications / attestations.

2.5.3.4. Security-Event Monitoring and Management: Continually monitor environments, systems, applications, processes and accounts for actual or potential security intrusions or violations. Promptly notify City according to BREACH NOTIFICATION / INCIDENT REPORTING (Section 2) below if suspicious conditions or activities are detected indicating an actual or potential security intrusion or violation. At City's option, cease, suspend, alter, modify or replace, as reasonably necessary, the products or services to be delivered or performed under the Agreement.

2.5.3.5. Share Responsibility Matrix: Cloud Service Consultants (CSP) shall operate following a documented, shared responsibility matrix that has been approved by the City.

3. BREACH NOTIFICATION / INCIDENT REPORTING

3.1. Interruption in Service Delivery. If any of the Agreement-required functions are interrupted, the Consultant will:

- Complete the recovery, resumption, and/or restoration activities as described in your DR plan to ensure continued compliance with all of the service levels set forth in this agreement.
- **Within 2 hours:** Using an agreed and documented notification procedures (such as runbook), notify City of Berkeley's Department of Information Technology within 2 hours of an interruption of an Agreement-required function, an initial report that includes the nature of the interruption and an estimate of the time it will take to return to agreement-required service levels.
- **Following restoration of Agreement-required functions to normal:** Provide City a complete report within 10 days, including a description of each Agreement-required function interrupted, the time required for recovery and return to Agreement-required service levels, Agreement-required products or services that were not provided or only partially provided as a result of the interruption, the specific corrective action taken, and the material effect, if any, on us and whether or not the DR Plan was adhered to and if not, what changes will be made to the Plan.

3.2. Suspected Security Incident. If you receive notice or other alert as to any actual or potential security intrusion or violation that will or could affect the City of Berkeley, its other vendors, or users of your application / service under the Agreement in matters exposing or impacting private and confidential information, including without limitation, City and its customers data and financial data (such as leak or loss), or service and system integrity and transactional accountability (such as failure/loss of fraud detection systems, data diddling, errors and omissions, etc.) or the City reputation risk status, complete the following. Notice or other alert includes any complaint or report you receive from a third party, including customers. Incidents include, without limitation, violations or potential violations of a federal or state law and industry regulations.

- Within 24 hours: Using the suspicious@cityofberkeley.info email address, notify City of Berkeley's Department of Information Technology of the alert and incident. In your notification, report to the City: (i) on the nature of the incident, (ii) estimated impact on us, and (iii) investigative action taken or planned.
- Within 3 business days after the initial incident report: Provide City with a written updated report that summarizes the results of the investigative action and corrective/remedial action taken.
- Upon completion of the investigation: Provide City with a final written report that gives a full accounting of the extent of the security intrusion or security violation; a description of any private and confidential information disclosed, destroyed, compromised or altered; specific corrective/remedial action taken; all supporting technical documentation that may include without limitation application and system network logs, and the cybersecurity impact on us and our systems.

3.3. Suspected Privacy Incident. If you discover or are notified of a Privacy or Information Security Incident relating to Customer Data, Consultant shall, to the extent not prohibited

by applicable law and at Consultant's cost and expense: (i) notify City of Berkeley of such Information Security Incident as set forth in section 3.2 (above), (ii) investigate such breach, (iii) inform City of Berkeley of the results of such investigation, and (iv) assist the City of Berkeley and State and Federal Agencies impacted by the breach with their reports, including but not limited to cyber suspicious activity reports (Cyber-SAR) and investigations, (v) assist City of Berkeley in maintaining the privacy and confidentiality of such information, (vi) cooperate in, support and assist City of Berkeley in making required breach notifications.

3.3.1. Consultant agrees to reasonably cooperate and coordinate with City of Berkeley concerning: (i) City's investigation, enforcement, monitoring, document preparation, notification requirements, efforts to prevent and mitigate, and reporting concerning Privacy and/or Information Security Incidents and Consultant's and City's compliance with Privacy and Information Security Laws; and (ii) any other activities or duties set forth under this Exhibit for which cooperation between Consultant and City of Berkeley may be reasonably necessary.

3.3.2. Any determination regarding the applicability of Information Security Laws or Privacy Laws to a Privacy or Information Security Incident and the scope of the obligations pursuant to such laws shall be within the reasonable discretion of City of Berkeley, and Consultant shall comply with any such reasonable determination.

3.3.3. When City of Berkeley elects to contact regulators or law enforcement agencies regarding an a Privacy or Information Security Incident, Consultant agrees to cooperate fully with such regulator or law enforcement agencies and any reasonable decision made by City of Berkeley regarding the scope and goals of any investigation undertaken by such regulator or law enforcement agencies.

3.3.4. The content of any filings, communications, notices, press releases or reports related to any Privacy Incident referencing City of Berkeley must be approved by City prior to any publication or communication thereof. If requested by City of Berkeley, Consultant shall provide notice to individuals who's Personal Information was affected by the Privacy Incident in a manner and format mutually agreed upon between Consultant and City, as well as any other third parties, such as regulators, law enforcement agencies and consumer reporting agencies.

3.3.5. Consultant further authorizes City of Berkeley, in the City's sole discretion and at the Consultant's sole expense, to provide notice of any reasonably required information and documents concerning any Privacy Incident, to individuals or third parties that may have been affected by the Privacy Incident, as well as to law enforcement authorities, regulators, and consumer reporting agency

3.4. Assistance in Litigation or Administrative Proceedings. Consultant shall make itself, and any subcontractors, employees, or agents assisting Consultant in the performance of its obligations under the Contract or Addendum, available to City of Berkeley, at no cost to City of Berkeley, to testify as witnesses, or otherwise, in the event of litigation or

administrative proceedings being commenced against City of Berkeley, its directors, officers, or employees based upon a claimed violation of applicable privacy and security laws and regulations except where Consultant or its subcontractor, employee or agent is a named adverse party.

4. CONSULTANT'S THIRD PARTIES

For Services performed by a Consultant's third-party (Party), Consultant will cause such Party to comply with this Agreement and the documentation herein. Consultant will remain solely liable for the acts or omissions of any such Party. Specifically, as part of this oversight responsibility:

4.1. Consultant must employ a vendor management and security due diligence program, reasonably approved by the City. Consultant must report to the City any proposed Party that cannot materially fulfil confidentiality or security requirements in this Agreement or the security documentation required by this section. City of Berkeley's cyber security and Department of Information Technology (DoIT) vendor management must review, on a case-by-case basis, each Party proposed by Consultant and approve or disapprove of the proposed Party in accordance with the terms of the Agreement.

4.2. Consultant must require each Party to comply with the requirements of the City Of Berkeley's Policies, Standards, and Guidelines and must monitor each such Party to determine compliance with same.

4.3. Consultant must monitor and provide ongoing oversight of the performance of each Party. Consultant will report to the City whenever there is a reasonably suspected security incident that could affect City Of Berkeley data or the performance of the Services, or that, in Consultant's reasonable judgment, could negatively affect City Of Berkeley's reputation.

5. RETURN OF CITY DATA

Within thirty (30) days of notification of termination of this Agreement, Consultant shall provide City with all City-owned data in dedicated data files suitable for importation into commercially available database software that is compatible with City's system. The dedicated data files will be comprised of City's data contained in Consultant's system. The structure of the relational database will be specific to the City's data and will not be representative of the proprietary Consultant's database.

At City's request, certify to City of Berkeley in writing, through a legal officer of Consultant, that you have returned or destroyed all City private and confidential information (including data residing in memory, on equipment or media).

END APPENDIX C

PRIVACY, SECURITY, AND RESILIENCE