

City and County of San Francisco Technology Marketplace

Software as a Service Term Sheet

This Software as a Service (“SaaS”) Term Sheet (“Term Sheet”) is attached, and incorporated as though fully set forth therein, to each Purchase Order for SaaS and Services issued under the OCA Technology Marketplace Master Agreement (“Agreement”). Capitalized terms used in this Term Sheet that are not otherwise defined have the meanings given them in the Agreement.

Now, THEREFORE, the parties agree as follows:

Article 1 Definitions

The following definitions apply to this Term Sheet:

1.1 “Acceptance” means notice from the City to Contractor that the SaaS Application meets the specifications and requirements contained in the Documentation and Agreement. City’s Acceptance shall be governed by the procedures set forth in Section 4.3.

1.2 “Acceptance Period” means the period allocated by City to test the SaaS Application to determine whether it conforms to the applicable specifications and, if appropriate, properly operates in the defined operating environment, is capable of running on a repetitive basis, and is otherwise in compliance with the service level obligations without failure.

1.3 “Agreement” means the Agreement to which this Term Sheet is attached and incorporated and this Term Sheet, including all attached appendices, and all applicable City Ordinances and Mandatory City Requirements, which are specifically incorporated into this Term Sheet by reference as provided herein.

1.4 “Authorized Users” means a person authorized by City to access the City’s Portal and use the SaaS Application, including any City employee, contractor or agent, or any other individual or entity authorized by City.

1.5 “Back-Up Environment” means Contractor’s back-up Data Center for the SaaS Services.

1.6 “City” or “the City” means the City and County of San Francisco, a municipal corporation, acting by and through both its Director of the Office of Contract Administration or the Director’s designated agent, hereinafter referred to as “Purchasing” and the requesting department.

1.7 “City Data” or “the City Data” means that data as described in Article 7 of this Term Sheet which includes, without limitation, all data collected, used, maintained, processed, stored, or generated by or on behalf of the City in connection with this Term Sheet, including data resulting from use of the SaaS Service. City Data includes, without limitation, Confidential Information.

1.8 “City Portal” means an electronic gateway to a secure entry point via Contractor’s Website that allows City and its Authorized Users to log in to an area where they can view and download information or request assistance regarding the SaaS Application and Services.

1.9 “City’s Project Manager” means the individual specified by the City pursuant to Section 4.2.1 hereof, as the Project Manager authorized to administer this Term Sheet on the City’s behalf.

1.10 “CMD” means the Contract Monitoring Division of the City.

1.11 “Confidential Information” means confidential City information including, but not limited to, Personally Identifiable Information (“PII”), protected health information (“PHI”), or individual financial information (collectively, “Proprietary or Confidential Information”) that is subject to local, state, or federal laws restricting the use and disclosure of such information. These laws include, but are not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act/California Consumer Privacy Act (Civil Code § 1798 et seq.); the California Confidentiality of Medical Information Act (Civil Code § 56 et seq.); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of part 164); and San Francisco Administrative Code Chapter 12M (Chapter 12M). Confidential Information includes, without limitation, City Data.

1.12 “Contractor” shall mean the Contractor with whom the City has entered into the Agreement and the entity to whom a Purchase Order is hereby issued for the purchase of SaaS and Services.

1.13 “Contractor Project Manager” means the individual specified by Contractor pursuant to Section 4.2.1 hereof, as the Project Manager authorized to administer this Term Sheet and the Agreement on Contractor’s behalf.

1.14 “Contractor’s Website” means the Website that provides Authorized User access to the SaaS Application Services.

1.15 “Data Breach” means any access, destruction, loss, theft, use, modification, or disclosure of City Data by an unauthorized party or that is in violation of this Term Sheet and the Agreement terms and/or applicable local, state, or federal law.

1.16 “Data Center(s)” means a physical location within the United States where Contractor (or its subcontractor) houses and operates the hardware (including computer servers, routers, and other related equipment) on which Contractor hosts on the Internet the SaaS Application and City Data pursuant to this Term Sheet and the Agreement.

1.17 “Deliverables” means Contractor’s work product resulting from the Services provided by Contractor to City during the course of Contractor’s performance of this Term Sheet and the Agreement, including without limitation, the work product described in the Purchase Order and Corresponding Documents.

1.18 “Deliverable Data” means Project Data that is identified in Appendix A to this Term Sheet, the Agreement, and/or accompanying Purchase Orders, and required to be delivered to the City.

1.19 “Disabling Code” means computer instructions or programs, subroutines, code, instructions, data, or functions (including but not limited to viruses, worms, and date bombs or time bombs) including, but not limited to, other programs, data storage, computer libraries, and programs that self-replicate without manual intervention; instructions programmed to activate at

a predetermined time or upon a specified event; and/or programs purporting to do a meaningful function, but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the City's access to the SaaS Services through Contractor's Website and/or Authorized User's processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

1.20 "Documentation" means technical publications provided by Contractor to City relating to use of the SaaS Application, such as reference, administrative, maintenance, and programmer manuals.

1.21 "End Users" means any Authorized User who accesses Contractor's Website and uses the SaaS Application and Services.

1.22 "Internet" means that certain global network of computers and devices commonly referred to as the "internet," including, without limitation, the World Wide Web.

1.23 "Mandatory City Requirements" means those City laws set forth in the San Francisco Municipal Code, including the duly authorized rules, regulations, and guidelines implementing such laws, which impose specific duties and obligations upon Contractor.

1.24 "Open Source Software" means software with either freely obtainable source code, a license for modification, or permission for free distribution.

1.25 "Party" or "Parties" means, respectively, the City and Contractor either individually or collectively.

1.26 "Performance Credit" means credit due to City by Contractor with regard to Contractor's service level obligations in appendices to this Term Sheet, the Agreement, and/or accompanying Purchase Orders.

1.27 "Personally Identifiable Information (PII)" means any information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that can reasonably be linked to an individual, such as medical, educational, financial, and employment information.

1.28 "Precedence" means that, notwithstanding the terms of any other document executed by the Parties as a part of this Term Sheet and the Agreement, the terms of this Term Sheet and the Agreement shall control over any discrepancy, inconsistency, gap, ambiguity, or conflicting terms set forth in any other Contractor pre-printed document.

1.29 "Project Data" means data that is first produced in the performance of this Term Sheet and the Agreement.

1.30 "Purchase Order" means the accompanying Purchase Order and any other corresponding documents ("Corresponding Documents") in response to a request for quote by City for the SaaS Services described in the Purchase Order. The Purchase Order is issued by City to Contractor pursuant to this Term Sheet and the Agreement. The Purchase Order and all Corresponding Documents are incorporated into this Term Sheet as though fully set forth herein.

1.31 “SaaS Application/SaaS Software/Software” means the licensed and hosted computer program and associated documentation, as listed in this Term Sheet and the Agreement and/or accompanying Purchase Orders, and any modification, Upgrades or modifications to the program(s), residing in Contractor’s servers that provides the SaaS Services that may be accessed by Authorized Users through the Internet. The SaaS Application may include Contractor provided Third-Party Software. All Software, revisions, and versions provided by Contractor shall be subject to the terms and conditions of this Term Sheet and the Agreement, including any amendments thereto.

1.32 “SaaS Application Patch” means an update to the SaaS Application comprised of code inserted (or patched) into the code of the SaaS Application, and which may be installed as a temporary fix between full releases of a SaaS Software Revision or SaaS Software Version. Such a patch may address a variety of issues including, without limitation, fixing a Software bug, installing new drivers, addressing new security vulnerabilities, addressing software stability issues, and upgrading the Software. SaaS Application Patches are included in the annual payments made by City to Contractor for the SaaS Services under this Term Sheet and the Agreement.

1.33 “SaaS Implementation and Training Services” means the services by which Contractor will implement all necessary Software configurations and modules necessary to make the SaaS Application available and accessible to City.

1.34 “SaaS Issue” means a problem with the SaaS Services identified by the City that requires a response by Contractor to resolve.

1.35 “SaaS Maintenance Services” means the activities to investigate, resolve SaaS Application and Services issues, and correct product bugs arising from the use of the SaaS Application and Services in a manner consistent with the published specifications and functional requirements defined during implementation.

1.36 “SaaS Services” means the Services performed by Contractor to host the SaaS Application to provide the functionality listed in the Documentation.

1.37 “SaaS Severity Level” means a designation of the effect of a SaaS Issue on the City. The severity of a SaaS Issue is initially defined by the City and confirmed by Contractor. Until the SaaS Issue has been resolved, the Severity Level may be raised or lowered based on Contractor’s analysis of impact to business.

1.38 “SaaS Software Error” means any failure of SaaS Software to conform in all material respects to the requirements of this Term Sheet and the Agreement or Contractor’s published specifications.

1.39 “SaaS Software Error Correction” means either a modification or addition that, when made or added to the SaaS Software, brings the SaaS Software into material conformity with the published specifications, or a procedure or routine that, when observed in the regular operation of the SaaS Software, avoids the practical adverse effect of such nonconformity.

1.40 “SaaS Software Revision” means an update to the current SaaS Software Version of the SaaS Software code that consists of minor enhancements to existing features and code corrections. SaaS Software Revisions are provided and included with the annual service payments made by City to Contractor for the SaaS Service.

1.41 “SaaS Software Version” means the base or core version of the SaaS Software that contains significant new features and significant fixes and is available to the City. SaaS Software Versions may occur as the SaaS Software architecture changes or as new technologies are developed. The nomenclature used for updates and upgrades consists of major, minor, build, and fix and these correspond to the following digit locations of a release, a, b, c, d, an example of which would be NCC 7.4.1.3, where the 7 refers to the major release, the 4 refers to the minor release, the 1 refers to the build, and the 4 refers to a fix. All SaaS Software Versions are provided and included as part of this Term Sheet and the Agreement upon request or approval from City for the upgrade.

1.42 “Scheduled SaaS Maintenance” means the time (in minutes) during the month, as measured by Contractor, in which access to the SaaS Services is scheduled to be unavailable for use by the City due to planned system maintenance and major version upgrades.

1.43 “Services” means the work performed by Contractor pursuant to accompanying Purchase Orders, Corresponding Documents, this Term Sheet, and the Agreement including all services, labor, supervision, materials, equipment, actions, and other requirements to be performed and furnished by Contractor under this Term Sheet and the Agreement.

1.44 “Successor Service Provider” means a new service provider, if any, selected by City in the event the SaaS Services are terminated under this Term Sheet and the Agreement.

1.45 “Term Sheet” means this document, the accompanying Purchase Order, all attached exhibits, and all applicable City Ordinances and Mandatory City Requirements in the Agreement between City and Contractor that are specifically incorporated into this Term Sheet by reference as provided herein.

1.46 “Third-Party Software” means the software described in the Agreement and/or accompanying Purchase Orders.

1.47 “Transition Services” means that assistance reasonably requested by City to effect the orderly transition of the SaaS Services, in whole or in part, to City or to Successor Service Provider.

Article 2 Term of the Term Sheet

2.1 **Term.** The term of this Term Sheet shall reflect the term of the SaaS Services set forth in the accompanying Purchase Order and Corresponding Documents, unless earlier terminated in accordance with the provisions of this Term Sheet or the Agreement.

Article 3 Financial Matters

3.1 **Calculation of Charges.** Contractor shall provide an invoice to City on a monthly basis for Goods delivered and/or Services completed in the immediately preceding month, unless a different schedule is set out in the accompanying Purchase Order and Corresponding Documents.

3.1.1 **SaaS Implementation and Training Services:** The breakdown of costs associated with the SaaS Implementation and Training Services appear in the accompanying Purchase Order and Corresponding Documents. In no event shall the amount for SaaS

Implementation and Training Services under this Agreement exceed the amount stated in the accompanying Purchase Order.

3.1.2 SaaS Application and Hosted Services: The breakdown of costs associated with the SaaS Application and Hosted Services appear in the accompanying Purchase Order and Corresponding Documents. In no event shall the amount for SaaS Application and Hosted Services under this Term Sheet and the Agreement exceed the amount stated in the Purchase Order. If there is an increase in annual SaaS Application and Hosted Services charges, Contractor shall give City written notice of such increase at least thirty (30) days prior to the expiration of the applicable SaaS Application and Hosted Services period. If not stated in the accompanying Purchase Order, annual SaaS Application and Hosted Services charges shall not increase more than five percent (5%) of the rate of the year immediately prior to such increase.

Article 4 SaaS Services and Resources

4.1 SaaS Licensed Software. Subject to the terms and conditions of this Term Sheet and the Agreement, Contractor hereby grants City and Authorized Users a renewable, irrevocable, non-exclusive, royalty-free, and worldwide license to access, display, and execute the SaaS Application and SaaS Services during the Term of this Term Sheet and the Agreement and any renewals thereof, if any.

4.1.1 Click-Wrap Disclaimer. No “click to accept” agreement that may be required for the City and/or Authorized Users’ access to the SaaS Services or Contractor’s Website and no “terms of use” or “privacy policy” referenced therein or conditioned for use of the SaaS Services or Contractor’s Website shall apply. Only the provisions of this Term Sheet and the Agreement as amended from time to time shall apply to City and/or Authorized Users for access thereto and use thereof. The Parties acknowledge that City and/or each Authorized User may be required to click “Accept” as a condition of access to the SaaS Services through Contractor’s Website, but the provisions of such “click to accept” agreement and other terms (including Terms of Use and Privacy Policy) referenced therein shall be null and void for City and/or each such Authorized User. The foregoing does not apply to the City’s own click-wrap agreements in the event the City chooses to have Contractor include terms of use, terms of service, privacy policies, or similar requirements drafted and approved by the City.

4.1.2 SaaS Application Title. City acknowledges that title to each SaaS Application and SaaS Services shall at all times remain with Contractor, and that City has no rights in the SaaS Application or SaaS Services except those expressly granted by this Term Sheet and the Agreement.

4.1.3 Authorized APIs. City shall be permitted to access and use Contractor’s SaaS Application Program Interfaces (APIs) when commercially available to develop and modify, as necessary, macros, and user interfaces for use with any existing or future City systems and infrastructure. For purposes of this Term Sheet and the Agreement, such development shall be deemed an authorized modification but will not be supported by Contractor unless provided for in this Term Sheet and the Agreement. Functionality and compatibility of City developed macros will be sole responsibility of City. Any such macros or user interfaces developed by City shall become the property of City. All flat-file exchanges will be over an encrypted file transport service (ftps/vsftpd/scp/sftp) to a secure private ftp site.

4.1.4 **Proprietary Markings.** City agrees not to remove or destroy any proprietary markings or proprietary legends placed upon or contained within the SaaS Application or any related materials or Documentation.

4.2 **Project Managers; Services Contractor Agrees to Perform.**

4.2.1 **Project Managers.** Contractor and City shall each designate a Project Manager, who shall be accessible by telephone throughout the duration of this Term Sheet and the Agreement and shall be available 9 a.m. to 5 p.m. (Pacific Standard Time), Monday through Friday, excluding City-designated holidays. These hours may be adjusted by mutual agreement of City and Contractor. Contractor shall use its best efforts to maintain the same Project Manager throughout the duration of this Term Sheet and the Agreement. However, if Contractor needs to replace its Project Manager, Contractor shall provide City with written notice thereof at least forty-five (45) days prior to the date the Project Manager shall be replaced. Notwithstanding the foregoing, Contractor will have the right to appoint temporary Project Managers in connection with short term unavailability, sick leave or reasonable vacations. Contractor shall notify City in advance of any such temporary appointments. City may require Contractor to replace its Project Manager, by giving Contractor notification thereof and City's objective reasons therefor.

4.2.2 **Services Contractor Agrees to Perform.** During the Term of this Term Sheet and the Agreement, Contractor will perform all of the Services set forth in this Term Sheet, the Agreement and/or accompanying Purchase Orders and the following:

(a) Provide telephone support for Authorized Users in the operation of the SaaS Application and Services.

(b) **Maintenance and Support.** Contractor shall provide Maintenance/Support in accordance with this Term Sheet, the Agreement, and/or accompanying Purchase Orders. Maintenance and Support Services include the provision of upgrades and a service desk, during the term of this Term Sheet and the Agreement for the SaaS Application(s).

(c) **Hosting.** Contractor shall provide hosting in accordance with Appendix A of this Term Sheet, including the following:

(i) **Hosting Infrastructure.** Contractor shall provide all hosting infrastructure, including, but not limited to, hardware, software and other equipment, at Contractor's hosting site as required to provide hosting and deliver the SaaS Application and Services.

(ii) **Security.** Contractor shall ensure that all electronic transmission or exchange of City Data will be encrypted using current industry standards. Contractor shall also ensure that all data exchanged shall be used expressly and solely for the purposes stated in this Term Sheet and the Agreement. City Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Contractor not involved in administration of this Term Sheet and the Agreement, unless otherwise permitted in this Term Sheet and the Agreement. Remote access to view City data by Contractor for development and technical support purposes from outside the United States is allowed as long as City Data remains hosted solely on systems residing in the continental United States.

(iii) **Access.** Contractor shall provide Authorized Users 24/7 access to the SaaS Application(s).

(iv) **Disaster Recovery and Business Continuity.** Contractor shall provide Disaster Recovery Services and assist with Business Continuity as described in Section 8.4 and Appendix C of this Term Sheet.

(d) **Service Level Obligations.** Contractor shall comply with the support (24/7 service desk) and Service Level Obligations described in Appendix D of this Term Sheet.

4.3 **Acceptance Testing; Document Delivery; Training.**

4.3.1 After City has obtained access to the SaaS Application and Services, and subsequent to each SaaS Software Version upgrade, revision and patch, City and Contractor shall conduct user Acceptance testing as outlined in this Term Sheet, the Agreement and accompanying Purchase Orders to verify that the SaaS Application and Services substantially conform to the specifications and City's requirements contained therein. In the event that the City determines that the SaaS Services do not meet such specifications, the City shall notify Contractor in writing, and Contractor shall modify or correct the SaaS Services so that it satisfies the Acceptance criteria. The date of Acceptance will be that date upon which City provides Contractor with written notice of satisfactory completion of Acceptance testing. If City notifies Contractor after the Acceptance Testing Period that the SaaS Services do not meet the Acceptance criteria outlined in this Term Sheet, the Agreement and accompanying Purchase Orders, then City shall be entitled to terminate the Purchase Order(s) in accordance with the procedures specified in the Agreement, and shall be entitled to a full refund of any fees paid as part of this Term Sheet and the Agreement prior to termination.

4.3.2 **Document Delivery.** Contractor will deliver completed Documentation in electronic format for the SaaS Application and Services at the time it gives City access to the SaaS Application and Services. The Documentation will accurately and completely describe the functions and features of the SaaS Application and Services, including all subsequent revisions thereto. The Documentation shall be understandable by a typical end user and shall provide Authorized Users with sufficient instruction such that an Authorized User can become self-reliant with respect to access and use of the SaaS Application and Services. City shall have the right to make any number of additional copies of the Documentation at no additional charge. The City may withhold its issuance of the notice of final Acceptance until City receives the completed Documentation.

4.3.3 **Warranty.** Contractor warrants to City that the Services will be performed with the degree of skill and care that is required by current, good, and sound professional procedures and practices, and in conformance with generally accepted professional standards prevailing at the time the Services are performed so as to ensure that all Services performed are correct and appropriate for the purposes contemplated in this Term Sheet.

4.3.4 **Subcontracting.** Notwithstanding Section 4.5.2 of the Agreement, all Subcontracts must incorporate the terms of Article 7 "Data and Security" of this Term Sheet, unless inapplicable.

Article 5 Indemnity and Warranties

5.1 Infringement Indemnification. If notified promptly in writing of any judicial action brought against City based on an allegation that City's use of the SaaS Application and Services infringes a patent, copyright, or any right of a third party or constitutes misuse or misappropriation of a trade secret or any other right in intellectual property (Infringement), Contractor will hold City harmless and defend such action at its own expense. Contractor will pay the costs and damages awarded in any such action or the cost of settling such action, provided that Contractor shall have sole control of the defense of any such action and all negotiations or its settlement or compromise, only if Contractor accepts the defense and hold harmless requirements without reservation, and provided, however, that Contractor shall not agree to any injunctive relief or settlement that obligates the City to perform any obligation, make an admission of guilt, fault or culpability, or incur any expense, without City's prior written consent, which shall not be unreasonably withheld or delayed. If notified promptly in writing of any informal claim (other than a judicial action) brought against City based on an allegation that City's use of the SaaS Application and/or Services constitutes Infringement, Contractor will pay the costs associated with resolving such claim and will pay the settlement amount (if any), provided that Contractor shall have sole control of the resolution of any such claim and all negotiations for its settlement, only if Contractor accepts the defense and hold harmless requirements without reservation, and provided, however, that Contractor shall not agree to any injunctive relief or settlement that obligates the City to perform any obligation, make an admission of guilt, fault or culpability, or incur any expense, without City's prior written consent, which shall not be unreasonably withheld or delayed. In the event a final injunction is obtained against City's use of the SaaS Application and Services by reason of Infringement, or in Contractor's opinion City's use of the SaaS Application and Services is likely to become the subject of Infringement, Contractor may at its option and expense: (a) procure for City the right to continue to use the SaaS Application and Services as contemplated hereunder, (b) replace the SaaS Application and Services with a non-infringing, functionally equivalent substitute SaaS Application and Services, or (c) suitably modify the SaaS Application and Services to make its use hereunder non-infringing while retaining functional equivalency to the unmodified version of the SaaS Application and Services. If none of these options is reasonably available to Contractor, then this Term Sheet and accompanying Purchase Order may be terminated at the option of either Party hereto and Contractor shall refund to City all amounts paid under this Term Sheet and accompanying Purchase Order for the license of such infringing SaaS Application and/or Services. Any unauthorized modification or attempted modification of the SaaS Application and Services by City or any failure by City to implement any improvements or updates to the SaaS Application and Services, as supplied by Contractor, shall void this indemnity unless City has obtained prior written authorization from Contractor permitting such modification, attempted modification, or failure to implement. Contractor shall have no liability for any claim of Infringement based on City's use or combination of the SaaS Application and Services with products or data of the type for which the SaaS Application and

Services was neither designed nor intended to be used, unless City has obtained prior written authorization from Contractor permitting such use.

5.2 Warranties of Contractor.

5.2.1 **Warranty of Authority; No Conflict.** Each Party warrants to the other that it is authorized to enter into this Term Sheet and the Agreement and that its performance of this Term Sheet and the Agreement will not conflict with any other agreement.

5.2.2 **Warranty of Performance.** Contractor warrants that when fully implemented, the SaaS Application to be configured and provided under this Term Sheet and the Agreement shall perform in accordance with the specifications applicable thereto. With respect to all Services to be performed by Contractor under this Term Sheet and the Agreement, Contractor warrants that it will use reasonable care and skill. All services shall be performed in a professional, competent, and timely manner by Contractor personnel appropriately qualified and trained to perform such services. In the event of a breach of the foregoing warranty relating to any service under this Term Sheet and the Agreement within twelve (12) months from the date of provision of such services, Contractor shall, at its sole cost and expense, re-perform such services.

5.2.3 **Compliance with Description of Services.** Contractor represents and warrants that the SaaS Application and Services specified in this Term Sheet and the Agreement and all updates and improvements to the SaaS Application and Services will comply in all material respects with the specifications and representations specified in the Documentation (including performance, capabilities, accuracy, completeness, characteristics, specifications, configurations, standards, functions, and requirements) as set forth (i) herein or in any amendment hereto, and (ii) the updates thereto.

5.2.4 **Title.** Contractor represents and warrants to City that it is the lawful owner or license holder of all Software, materials, and property identified by Contractor as Contractor-owned and used by it in the performance of the SaaS Services contemplated hereunder and has the right to permit City access to or use of the SaaS Application and Services and each component thereof. To the extent that Contractor has used Open Source Software (“OSS”) in the development of the SaaS Application and Services, Contractor represents and warrants that it is in compliance with any applicable OSS license(s) and is not infringing.

5.2.5 **Disabling Code.** Contractor represents and warrants that the SaaS Application and Services, and any information, reports or other materials provided to Authorized Users as a result of the operation of the SaaS Application and Services, including future enhancements and modifications thereto, shall be free of any Disabling Code.

5.2.6 **Warranty of Suitability for Intended Purpose.** Contractor warrants that the SaaS Application and Services will be suitable for the intended purpose of this Term Sheet and the Agreement.

Article 6 Termination; Disposition of Content; Survival

6.1 **Termination for Cause and/or Convenience.** City shall have the right, without further obligation or liability to Contractor:

6.1.1 To immediately terminate this Term Sheet and the accompanying Purchase Order if Contractor commits any breach of this Term Sheet and the accompanying Purchase Order or default (see Section 8.2 of the Agreement) and fails to remedy such breach or default within ten (10) days after written notice by City of such breach (10-day cure period), in which event, Contractor shall refund to City all amounts paid under this Term Sheet and the accompanying Purchase Order for the SaaS Application and/or Services in the same manner as if City ceased to use the SaaS Application due to infringement under Section 4.1 of this Term Sheet. At City's sole election, the 10-day cure period will *not* apply to termination for data breach and/or breach of confidentiality; or

6.1.2 To terminate this Term Sheet and the accompanying Purchase Order upon thirty (30) days prior written notice for City's convenience and without cause, provided that except for termination due to an uncured breach as set forth in this Section and in the event of Infringement, City shall not be entitled to a refund of any amounts previously paid under this Term Sheet and the accompanying Purchase Order.

6.2 **Bankruptcy.** In the event that Contractor shall cease conducting business in the normal course, become insolvent, make a general assignment for the benefit of creditors, suffer or permit the appointment of a receiver for its business or assets or shall avail itself of, or become subject to, any proceeding under the Federal Bankruptcy Act or any other statute of any state relating to insolvency or the protection of rights of creditors, then at City's option this Term Sheet and the Agreement shall terminate and be of no further force and effect. Upon termination of this Term Sheet and the accompanying Purchase Order pursuant to this Section, Contractor shall within forty-eight (48) hours return City's Data in an agreed-upon machine readable format. Once Contractor has received written confirmation from City that City's Data has been successfully transferred to City, Contractor shall within thirty (30) calendar days clear, purge, or physically destroy all City Data from its hosted servers or files, and provide City with written certification within five (5) calendar days that such clear, purge, and/or physical destruction has occurred. Secure disposal shall be accomplished by "clearing," "purging," or "physical destruction" in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 or most current industry standard.

6.3 **Transition Services and Disposition of City Data.** Notwithstanding anything to the contrary set forth in the accompanying Purchase Order and Corresponding Documents, upon expiration or termination of the SaaS Services under this Term Sheet:

6.3.1 Contractor may immediately discontinue the SaaS Services and City shall immediately cease accessing the SaaS Application and Services. Contractor shall within five (5) calendar days of the expiration or termination of the SaaS Services return City's data in an agreed-upon machine readable format. This provision shall also apply to all City Data that is in the possession of subcontractors, agents, or auditors of Contractor. Such data transfer shall be done at no cost to the City. Once Contractor has received written confirmation from City that City's Data has been successfully transferred to City, Contractor shall within thirty (30) calendar days clear, purge, or physically destroy all City Data from its hosted servers or files, and provide City with written certification within five (5) calendar days that such clear or purge, and/or physical destruction has occurred. Secure disposal shall be accomplished by "clearing," "purging," or "physical destruction" in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 or most current industry standard.

6.3.2 Contractor shall provide to City and/or Successor Service Provider assistance requested by City to effect the orderly transition of the SaaS Services, in whole or in part, to City or to Successor Service Provider. During the transition period, SaaS and City Data access shall continue to be made available to City without alteration. Such Transition Services shall be provided on a time and materials basis if the City opts to return to its own servers or City chooses a Successor Service Provider. Transition costs may include: (a) developing a plan for the orderly transition of the terminated SaaS Services from Contractor to Successor Service Provider; (b) if required, transferring the City Data to Successor Service Provider; (c) using commercially reasonable efforts to assist City in acquiring any necessary rights to legally and physically access and use any third-party technologies and documentation then being used by Contractor in connection with the Services; (d) using commercially reasonable efforts to make available to City, pursuant to mutually agreeable terms and conditions, any third-party services then being used by Contractor in connection with the SaaS Services; and (e) such other activities upon which the Parties may agree. Notwithstanding the foregoing, should City terminate this Term Sheet, City may elect to use the Services for a period of no greater than six (6) months from the date of termination at a reduced rate of twenty (20%) percent off of the then-current Services Fees for the terminated Services. All applicable terms and conditions of this Term Sheet shall apply to the Transition Services. This Section 6.3.2 shall survive the termination of this Term Sheet.

6.4 **Survival.** This Section and the following Sections of this Term Sheet listed below, shall survive termination or expiration of this Term Sheet and the Agreement:

6.5	Data Rights
-----	-------------

6.5 Data Rights

6.5.1 Preexisting Data of each Party that will be included as a Deliverable under this Term Sheet and the Agreement will be identified in the Purchase Order and Corresponding Documents. Preexisting Data of the City may only be used by Contractor for purposes of the scope of work of this Term Sheet, unless such data is otherwise publicly available.

6.5.2 The City shall have the unrestricted right to use the Deliverable Data and delivered Project Data, including all Preexisting Data provided as a Deliverable under this Term Sheet and the Agreement.

Article 7 Data and Security

7.1 City Data

7.1.1 **Ownership of City Data.** The Parties agree that as between them, all rights, including all intellectual property rights, in and to the City Data and any derivative works of the City Data is the exclusive property of the City. Contractor warrants that the SaaS Application does not maintain, store, or export the City Data using a database structure, data model, entity relationship diagram, or equivalent.

7.1.2 **Use of City Data.** Contractor agrees to hold City Data received from, or created or collected on behalf of, the City in strictest confidence. Contractor shall not use or disclose City's Data except as permitted or required by this Term Sheet, the Agreement, or as

otherwise authorized in writing by the City. Any work using or sharing, or storage of City's Data outside the United States is subject to prior written authorization by the City. Access to City's Confidential Information must be strictly controlled and limited to Contractor's staff assigned to this project on a need-to-know basis only. Contractor is provided a limited non-exclusive license to use the City Data solely for performing its obligations under the Agreement and not for Contractor's own purposes or later use. Nothing herein shall be construed to confer any license or right to the City Data, including user tracking and exception City Data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third-party. Unauthorized use of City Data by Contractor, subcontractors, or other third-parties is prohibited. For purpose of this requirement, the phrase "unauthorized use" means the data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any purpose that is not explicitly authorized other than security or service delivery analysis.

7.1.3 Access to and Extraction of City Data. City shall have access to City Data twenty-four (24) hours a day, seven (7) days a week. The SaaS Application shall be capable of creating a digital, reusable copy of the City Data, in whole and in parts, as a platform independent and machine-readable file. Such file formats include, without limitation, plain text files such as comma-delimited tables, extensible markup language, and javascript object notation. City Data that is stored in binary formats, including without limitation portable document format, JPEG, and portable network graphics files, shall instead be reproducible in the same format in which it was loaded into the SaaS Application. This reusable copy must be made available in a publicly documented and non-proprietary format, with a clearly-defined data structure and a data dictionary for all terms of art contained in the data. For purposes of this section, non-proprietary formats include formats for which royalty-free codecs are available to End Users. Contractor warrants that City shall be able to extract City Data from the SaaS Application on demand, but no later than twenty-four (24) hours of City's request, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees to Contractor).

7.1.4 Backup and Recovery of City Data. As a part of the SaaS Services, Contractor is responsible for maintaining a backup of City Data and for an orderly and timely recovery of such data in the event of data corruption or interruption of the SaaS Services. Unless otherwise described in this Term Sheet, the Agreement and/or accompanying Purchase Orders, Contractor shall maintain a contemporaneous backup of City Data that can be recovered within the requirements in this Term Sheet and the Agreement and as outlined in this Term Sheet, the Agreement, and/or accompanying Purchase Orders and maintaining the security of City Data as further described herein. Contractor's backup of City Data shall not be considered in calculating storage used by City.

7.1.5 Data Breach; Loss of City Data. Notwithstanding anything to the contrary set forth in the Agreement and accompanying Purchase Orders, in the event of any Data Breach, act, SaaS Software Error, omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of City Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of City Data, Contractor shall, as applicable:

(a) Notify City immediately following discovery, but no later than twenty-four (24) hours, of becoming aware of such occurrence or suspected occurrence. Contractor's report shall identify:

- (i) the nature of the unauthorized access, use, or disclosure;
- (ii) the Confidential Information accessed, used, or disclosed;
- (iii) the person(s) who accessed, used, disclosed, and/or received protected information (if known);
- (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized access, use, or disclosure; and
- (v) what corrective action Contractor has taken or will take to prevent future unauthorized access, use, or disclosure.

(b) In the event of a suspected Breach, Contractor shall keep the City informed regularly of the progress of its investigation until the uncertainty is resolved;

(c) Contractor shall coordinate with the City in its breach response activities including without limitation:

- (i) Immediately preserve any potential forensic evidence relating to the breach, and remedy the breach as quickly as circumstances permit;
- (ii) Promptly (within two (2) business days) designate a contact person to whom the City will direct inquiries, and who will communicate Contractor responses to City inquiries;
- (iii) As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore City service(s) as directed by the City, and undertake appropriate response activities;
- (iv) Provide status reports to the City on Data Breach response activities, either on a daily basis or a frequency approved by the City;
- (v) Make all reasonable efforts to assist and cooperate with the City in its Breach response efforts;
- (vi) Ensure that knowledgeable Contractor staff are available on short notice, if needed, to participate in City-initiated meetings and/or conference calls regarding the Breach; and
- (vii) Cooperate with City in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by City.

(d) In the case of personally identifiable information (PII) or protected health information (PHI), at City's sole election, (a) notify the affected individuals as soon as

practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or
(b) reimburse City for any costs in notifying the affected individuals;

(e) In the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no fewer than twenty-four (24) months following the date of notification to such individuals;

(f) Perform or take any other actions required to comply with applicable law as a result of the occurrence;

(g) Recreate lost City Data in the manner and on the schedule set by City without charge to City; and

(h) Provide to City a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence.

(i) Notification to affected individuals, as described above, shall comply with applicable law, be written in plain language, and contain (at the City's election) information that may include: name and contact information of Contractor's (or City's) representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor.

(j) Contractor shall retain and preserve City Data in accordance with the City's instruction and requests, including without limitation any retention schedules and/or litigation hold orders provided by the City to Contractor, independent of where the City Data is stored.

(k) City shall conduct all media communications related to such Data Breach, unless in its sole discretion, City directs Contractor to do so.

7.2 Proprietary or Confidential Information

7.2.1 Proprietary or Confidential Information of City. Contractor understands and agrees that, in the performance of the work or Services under this Term Sheet and the Agreement may involve access to City Data that is Confidential Information. Contractor and any subcontractors or agents shall use Confidential Information only in accordance with all applicable local, state and federal laws restricting the access, use, and disclosure of Confidential Information and only as necessary in the performance of this Term Sheet and the Agreement. Contractor's failure to comply with any requirements of local, state, or federal laws restricting access, use, and disclosure of Confidential Information shall be deemed a material breach of this Term Sheet and the Agreement, for which City may terminate this Term Sheet and the Agreement. In addition to termination or any other remedies set forth in this Term Sheet and the Agreement or available in equity or law, the City may bring a false claim action against Contractor pursuant to Chapters 6 or 21 of the Administrative Code, or debar Contractor. Contractor agrees to include all of the terms and conditions regarding Confidential Information

contained in this Term Sheet and the Agreement in all subcontractor or agency contracts providing Services under this Term Sheet and the Agreement.

7.2.2 Obligation of Confidentiality. Subject to San Francisco Administrative Code Section 67.24(e), any state open records or freedom of information statutes, and any other applicable laws, Contractor agrees to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, otherwise dispose of, give, or disclose such Confidential Information to third-parties other than its employees, agents, or authorized subcontractors who have a need to know in connection with this Term Sheet and the Agreement or to use such Confidential Information for any purposes whatsoever other than the performance of this Term Sheet and the Agreement. Contractor agrees to advise and require its respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential.

7.2.3 Nondisclosure. Contractor agrees and acknowledges that it shall have no proprietary interest in any proprietary or Confidential Information and will not disclose, communicate or publish the nature or content of such information to any person or entity, nor use, except in connection with the performance of its obligations under this Term Sheet and the Agreement or as otherwise authorized in writing by the disclosing Party, any of the Confidential Information it produces, receives, acquires, or obtains from the disclosing Party. Contractor shall take all necessary steps to ensure that the Confidential Information is securely maintained. Contractor's obligations set forth herein shall survive the termination or expiration of this Term Sheet and the Agreement. In the event Contractor becomes legally compelled to disclose any of the Confidential Information, it shall provide the City with prompt notice thereof and shall not divulge any information until the City has had the opportunity to seek a protective order or other appropriate remedy to curtail such disclosure. If such actions by the disclosing Party are unsuccessful, or the disclosing Party otherwise waives its right to seek such remedies, the receiving Party shall disclose only that portion of the Confidential Information that it is legally required to disclose.

7.2.4 Litigation Holds. Contractor shall retain and preserve City Data in accordance with the City's instruction and requests, including without limitation any retention schedules and/or litigation hold orders provided by the City to Contractor, independent of where the City Data is stored.

7.2.5 Cooperation to Prevent Disclosure of Confidential Information. Contractor shall use its best efforts to assist the City in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, Contractor shall advise the City immediately in the event Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Term Sheet and the Agreement, and Contractor will cooperate with the City in seeking injunctive or other equitable relief against any such person.

7.2.6 Remedies for Breach of Obligation of Confidentiality. Contractor acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the City, which damage may be inadequately compensable in the form of monetary damages. Accordingly, City may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available, to include, at the sole election of City, the immediate termination of this Term Sheet and/or the Agreement, without liability to City.

7.2.7 Surrender of Confidential Information upon Termination. Upon termination of this Term Sheet and/or the Agreement, including but not limited to expiration of the term, early termination or termination for convenience, Contractor shall, within five (5) calendar days from the date of termination, return to City any and all Confidential Information received from the City, or created or received by Contractor on behalf of the City, which are in Contractor's possession, custody, or control. The return of Confidential Information to City shall follow the timeframe and procedure described further in this Term Sheet (Article 5).

7.2.8 Data Security. To prevent unauthorized access of City Data,

(a) Contractor shall at all times during the term of this Term Sheet and the Agreement provide and maintain up-to-date security with respect to (i) the Services, (ii) Contractor's Website, (iii) Contractor's physical facilities, (iv) Contractor's infrastructure, and (v) Contractor's networks.

(b) Contractor shall provide security for its networks and all Internet connections consistent with industry best practices, and will promptly install all patches, fixes, upgrades, updates, and new versions of any security software it employs.

(c) Contractor will maintain appropriate safeguards to restrict access to City's Data to those employees, agents, or service providers of Contractor who need the information to carry out the purposes for which it was disclosed to Contractor.

(d) For information disclosed in electronic form, Contractor agrees that appropriate safeguards include electronic barriers (e.g., most current industry standard encryption for transport and storage, such as the National Institute of Standards and Technology's Internal Report 7977 or Federal Information Processing Standards [FIPS] 140-2 [Security Requirements for Cryptographic Modules] or FIPS-197 or successors, intrusion prevention/detection or similar barriers) and secure authentication (e.g., password protected) access to the City's Confidential Information and hosted City Data.

(e) For information disclosed in written form, Contractor agrees that appropriate safeguards include secured storage of City Data.

(f) City Data shall be encrypted at rest and in transit with controlled access.

(g) Contractor will establish and maintain any additional physical, electronic, administrative, technical, and procedural controls and safeguards to protect City Data that are no less rigorous than accepted industry practices (including, as periodically amended or updated, the International Organization for Standardization's standards: ISO/IEC 27001:2005 – Information Security Management Systems – Requirements and ISO-IEC 27002:2005 – Code of Practice for International Security Management, NIST Special Publication 800-53 Revision 4 or its successor, NIST Special Publication 800-18 or its successor, the Information Technology Library (ITIL) standards, the Control Objectives for Information and related Technology (COBIT) standards or other applicable industry standards for information security), and shall ensure that all such controls and safeguards, including the manner in which Confidential Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Term Sheet and the Agreement.

(h) Contractor warrants to the City compliance, in performing its obligations hereunder, with the following (as periodically amended or updated) as applicable:

- (i) The California Information Practices Act/California Consumer Privacy Act (Civil Code §§ 1798 et seq);
- (ii) The European General Data Protection Regulation (“GDPR”);
- (iii) Relevant security provisions of the Internal Revenue Service (IRS) Publication 1075, including the requirements that Data not traverse networks located outside of the United States;
- (iv) Relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCI DSS), including the PCI DSS Cloud Computing Guidelines;
- (v) Relevant security provisions of the Social Security Administration (SSA) Document Electronic Information Exchange Security Requirement and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration;
- (vi) Relevant security provisions of the Criminal Justice Services (CJIS) Security policy;
- (vii) Relevant security provisions of the Medi-Cal Privacy and Security Agreement between the California Department of Health Care Services and the County of San Francisco.

7.2.9 **Data Privacy and Information Security Program.** Without limiting Contractor’s obligation of confidentiality as further described herein, Contractor shall establish and maintain a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (i) ensure the security and confidentiality of the City Data; (ii) protect against any anticipated threats or hazards to the security or integrity of the City Data; (iii) protect against unauthorized disclosure, access to, or use of the City Data; (iv) ensure the proper disposal of City Data; and (v) ensure that all of Contractor’s employees, agents, and subcontractors, if any, comply with all of the foregoing.

7.2.10 **City’s Right to Termination for Deficiencies.** City reserves the right, at its sole election, to immediately terminate this Term Sheet and the Agreement, without limitation and without liability, if City reasonably determines that Contractor fails or has failed to meet its obligations under this Article 7.

7.2.11 **Data Transmission.** Contractor shall ensure that all electronic transmission or exchange of system and application data with City and/or any other parties expressly designated by City shall take place via encrypted secure means (e.g. HTTPS, SFTP, or most current industry standard established by NIST). Contractor shall also ensure that all data exchanged shall be used expressly and solely for the purposes enumerated in this Term Sheet and the Agreement. Data shall not be distributed, repurposed or shared across other applications,

environments, or business units of Contractor. Contractor shall ensure that no City Data of any kind shall be copied, modified, destroyed, deleted, transmitted, exchanged, or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by City. Contractor is prohibited from accessing City Data from outside the continental United States.

7.3 American Institute of Certified Public Accounts (AICPA) Audit Reports.

7.3.1 Contractor shall provide to City, on an annual basis, an SSAE 18, SOC 2, Type 2 Report, and an SSAE 18, SOC 1, Type 2 Audit Report, to be conducted by an independent third party (“Audit Reports”) (if Contractor is using a hosting service provider, Contractor shall provide such Audit Reports it receives from its service provider or providers) as follows: (a) the Audit Reports shall include a 365 day (12-month) testing period; and (b) the Audit Reports shall be available to City no later than thirty (30) days after they are received by Contractor. If Contractor receives a so-called “negative assurance opinion,” or the annual Audit Report finds a material data privacy or information security issue, Contractor shall notify City of such opinion within three (3) days of receipt by Contractor. Contractor shall implement reasonably required safeguards as identified by any audit of Contractor’s data privacy and information security program or promptly notify City in writing if Contractor is unable to implement mitigation measures to address the issue(s). Upon any such notification, City shall have the right, without further obligation or liability to Contractor, to terminate this Term Sheet and the Agreement. Any failure by Contractor to comply with this Section shall be a material breach of this Term Sheet and the Agreement.

7.3.2 **Audit of Contractor’s Policies.** Contractor agrees to make its policies, procedures and practices regarding Data Security available to City, if needed, and agrees that City reserves the rights including, but not limited to, making a site visit, scanning for malicious codes, and hiring a third-party to perform a security audit if City determines that the Audit Report is unsatisfactory.

7.3.3 **Information Security Audits.** Contractor must contract with an independent third party to perform yearly information security audits of their primary and backup Data Centers. The annual audits must include an outside penetration/vulnerability test, and internal penetration and vulnerability tests with the third-party directly on the internal network. The summary results of the audits must be shared with the City. All audit findings must be remedied.

7.3.4 **Audit Findings.** Contractor shall implement reasonably required safeguards as identified by City or by any audit of Contractor’s data privacy and information security program.

Article 8 Force Majeure

8.1 **Liability.** No Party shall be liable for delay in the performance of its obligations under this Term Sheet if and to the extent such delay is caused, directly or indirectly, by: fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, or any other cause beyond the reasonable control of such Party (a “Force Majeure Event”). In the case of a Force Majeure Event, Contractor shall immediately commence disaster recovery services as described in Section 7.4 of this Term Sheet.

8.2 **Duration.** In a Force Majeure Event, the non-performing Party shall be excused from further performance or observance of the obligation(s) so affected for as long as such circumstances prevail and such Party continues to use its best efforts to recommence performance or observance whenever and to whatever extent possible without delay. Any Party so delayed in its performance shall immediately notify the Party to whom performance is due by telephone (to be confirmed in writing within two (2) days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

8.3 **Effect.** If a Force Majeure Event substantially prevents, hinders, or delays performance of the Services as critical for more than fifteen (15) consecutive days, then at City's option: (i) City may terminate any portion of this Term Sheet and the accompanying Purchase Order so affected and the charges payable hereunder shall be equitably adjusted to reflect those terminated Services; or (ii) City may terminate this Term Sheet and the accompanying Purchase Order without liability to City or Contractor as of a date specified by City in a written notice of termination to Contractor. Contractor shall not have the right to any additional payments from City for costs or expenses incurred by Contractor as a result of any force majeure condition that lasts longer than three (3) days.

8.4 **Disaster Recovery.** In the event of a disaster, as defined below, Contractor shall provide disaster recovery services in accordance with the provisions of the disaster recovery plan set forth in this Term Sheet, the Agreement, and/or accompanying Purchase Orders. Notwithstanding Section 8.1, a Force Majeure Event shall not excuse Contractor of its obligations for performing disaster recovery services as provided in this Section. In the event that a disaster occurs and Contractor fails to restore the hosting services within twenty-four (24) hours of the initial disruption to Services, City may, in its discretion, deem such actions to be a material default by Contractor incapable of cure, and City may immediately terminate this Term Sheet and the accompanying Purchase Order. For purposes of this Term Sheet, a "disaster" shall mean an interruption in the hosting services or the inability of Contractor to provide City with the SaaS Application and hosting services for any reason that could not be remedied by relocating the SaaS Application and hosting services to a different physical location outside the proximity of its primary Data Center.

Article 9 Appendices

9.1 **Additional Appendices.** The following appendices are hereby attached and incorporated into this Term Sheet and the Agreement as though fully set forth herein and together form the complete agreement between the Parties:

Appendices:

- A. SaaS Application & Hosting Services
- B. Service Level Obligations
- C. Disaster Recovery Plan

Appendix A
SaaS Application & Hosting Services: Minimum Requirements

The following represent minimum requirements that Contractor shall meet or exceed with regard to its SaaS Application & Hosting Services.

- I. Description of the SaaS Application and Hosted Services**
- II. SaaS Data Centers**
- III. SaaS Maintenance Services**
- IV. City Responsibilities**
- V. Technical Support & Training**

I. Description of the SaaS Application and Hosted Services: “SaaS Application and Hosted Services” are set forth in the Term Sheet, the Agreement, and/or accompanying Purchase Orders.

A. Software: Use of Contractor’s Software operating on hosted equipment located at Contractor’s facility and/or any Data Center as further outlined in the Term Sheet, the Agreement, and/or accompanying Purchase Orders.

B. Third-Party Software:

1. Providing certain third-party software required to operate the SaaS Software and other bundled third-party software packages required to support the operation of the SaaS Software.
2. Inclusion of regular Software and Contractor-supplied third-party software updates, patches and fixes as scheduled by Contractor.

C. Remote Software: Contractor shall provide access to and use of a remote software tool for City management of Authorized Users, access rights and other similar role-based controls as they pertain to the SaaS Services. Method will be published through Contractor portal and be made available to Authorized Users with elevated privileges.

D. Back-Up of City’s Data:

1. Contractor shall provide up to thirty-six (36) months of on-line hourly data retention for SaaS Software operation and functionality.
2. Contractor shall provide incremental City Data backups at a minimum of every four (4) hours to an off-site location other than the primary hosting center.
3. Contractor shall provide weekly, off-site backups with a duration that matches the agreed-upon backup schedule and retention to a location other than the primary hosting center. Off-site backups to include previous eight (8) weeks.

E. SaaS Environments: The SaaS Application and Hosted Services shall be hosted in a certified and secure Tier-3 data hosting center.

1. A single Back-up Environment available as needed to serve as the backup or “failover” environment for the SaaS and Hosted Services
2. A single test environment available to the City and Contractor for the evaluation and eventual promotion of SaaS Software updates, patches, fixes or otherwise deemed tests. Test Environment shall perform at 50% or better of production environment.

F. Reporting: Contractor shall provide electronic notification within 2 hours of discovery and subsequent monthly reporting of any incidents or breaches that had occurred within the environment or to the hosted application. In the event of a breach, Contractor shall follow the procedures set forth in Article 7 of this Term Sheet.

G. Availability of SaaS Services: Contractor (or its Hosting Service contractor) shall host the SaaS Services on computers owned or controlled by Contractor (or its contractor) and shall provide the City with access to both a production environment with SaaS Application and data and a test environment with SaaS Application via Internet-access to use according to the terms herein.

1. **Hosted System Uptime:** Other than Scheduled SaaS Maintenance Services as outlined in Section III, emergency maintenance described below, Force Majeure as described in this Term Sheet and lack of Internet availability as described below, Contractor shall provide uptime to the SaaS Application and Hosted Service to achieve a 99.9% Service Level Availability.

2. **Scheduled SaaS Maintenance**

i. Contractor shall conduct Scheduled SaaS Maintenance during the following hours: Saturdays between 12 AM (Pacific Time) and 8 AM (Pacific Time), with the same exclusions noted in subsection 1, above.

ii. Scheduled SaaS Maintenance shall not exceed an average of 4 hours per month over a twelve (12) month period except for major scheduled upgrades.

3. **Unscheduled SaaS Maintenance.** Contractor shall use commercially reasonable efforts to prevent more than one (1) hour of continuous down time during business hours in any month for which unscheduled SaaS maintenance is required. If Contractor fails to meet this obligation for a period of three (3) successive calendar months, Contractor shall furnish City with a Performance Credit in the amount of 10% of the Services Fees (as calculated on a monthly basis for the reporting month).

4. **Emergency Maintenance.** If Force Majeure Events or emergencies arise or continue, Contractor shall be entitled to take any actions that Contractor, in good faith, determines is necessary or advisable to prevent, remedy, mitigate, or otherwise address actual or potential harm, interruption, loss, threat, security, or like concern to any of the SaaS systems or

the SaaS Software. Such emergency maintenance may include, but is not limited to: analysis, testing, repair, maintenance, re-setting and other servicing of the hardware, cabling, networks, software and other devices, materials, and systems through which access to and/or use of the SaaS Software by City is made available. Contractor shall endeavor to provide advance written notice of such emergency maintenance to City as soon as is reasonably possible.

5. **Notice of Unavailability:** In the event there will be more than thirty (30) minutes down time of any SaaS or Hosted Service components for any reason including, but not limited to, Scheduled SaaS Maintenance or emergency maintenance, Contractor shall provide notice to users by posting a web page that indicates that the site is temporarily unavailable and to please come back later. Contractor shall also provide advanced e-mail notice to the City email(s) to which the license(s) are registered, which will include at least a brief description of the reason for the down time and an estimate of the time when City can expect the site to be up and available.

H. Changes in Functionality. During the term of the Term Sheet and the Agreement, Contractor shall not reduce or eliminate functionality in SaaS Services. Where Contractor has reduced or eliminated functionality in SaaS Services, City, in its sole election, shall: (i) have, in addition to any other rights and remedies under the Term Sheet and the Agreement or at law, the right to immediately terminate the Term Sheet and the Agreement and be entitled to a return of any prepaid fees; or (ii) determine the value of the reduced or eliminated functionality and Contractor shall immediately adjust the Services fees accordingly on a prospective basis. Where Contractor increases functionality in the SaaS Services, such functionality shall be provided to City without any increase in the Services fees.

II. SaaS Data Centers

A. Control: The method and means of providing the Services shall be under the exclusive control, management, and supervision of Contractor, giving due consideration to the requests of City. Contractor, or any previously approved subcontractor, shall provide the Services (including data storage) solely from within the continental United States and on computing and data storage devices residing in the United States.

B. Data Center Standards.

Contractor's Data Centers shall have fully redundant and diverse network paths to City endpoints. Data Centers shall be located in geographically different seismic zones characterized by the lowest predicted chance of damage as defined by the US Geological Survey Earthquake Hazards Program.

Environmental systems must monitor/detect temperature, humidity, fluid leaks, and fire/smoke/particulate and have accompanying suppression systems. Fire suppression systems should be dry pipe. Power should be fully conditioned to avoid spikes and other aberrations that can damage equipment. Temporary power units, such as generators, must be in place to support SaaS Services in the event of a power outage for up to three (3) calendar days, and fuel replenishment contracts must be in place to keep temporary power operational for longer periods.

C. Location: The location of the approved Data Centers that will be used to host the SaaS Application will be clearly identified in the Agreement and/or accompanying Purchase Orders. They shall include a Primary Tier 3 Data Center and a Back-up Tier 2 Data Center.

D. Replacement Hosted Provider: In the event Contractor changes the foregoing Hosted Provider, Contractor shall provide City with prior written notice of said change and disclose the name and location of the replacement Hosted Provider. The replacement Hosted Provider shall be a reputable Hosted Provider comparable to Contractor's current Hosted Provider, and said replacement Hosted Provider shall be located within the United States. If applicable, the replacement Hosted Provider shall perform a SSAE 18, SOC 2, Type 2 Report and/or an SSAE 18, SOC 1, Type 2 Audit Report at least annually, in accordance with Section 13.3 of the Term Sheet.

E. Notice of Change: If the location of the Data Center used to host the SaaS Application is changed, Contractor shall provide City with written notice of said change at least sixty (60) days prior to any such change taking place. Contractor shall disclose the address of the new facility, which shall be within the United States. The Data Centers referenced above are subcontractors that must be approved by City.

F. Subcontractors. Contractor shall not enter into any subcontracts for the performance of the Services, or assign or transfer any of its rights or obligations under the Term Sheet and the Agreement, without City's prior written consent and any attempt to do so shall be void and without further effect and shall be a material breach of the Term Sheet and the Agreement. Contractor's use of subcontractors shall not relieve Contractor of any of its duties or obligations under the Term Sheet and the Agreement.

III. SaaS Maintenance Services.

A. The SaaS Software maintained under this Term Sheet and the Agreement shall be the SaaS Software set forth in the Term Sheet, Agreement, and/or accompanying Purchase Orders.

B. The following SaaS Maintenance Services are included as part of the Term Sheet and the Agreement:

1. **Contractor Software Version Upgrades, Software Revisions and Patches.** Contractor shall provide and implement all SaaS Software Version upgrades, SaaS Software Revisions, and SaaS Software Patches to ensure: (a) that the functionality of the SaaS Software and Services, as described in the Documentation, is available to Authorized Users; (b) that the functionality of the SaaS Software and Services is in accordance with the representations and warranties set forth herein including, but not limited to, the SaaS Software and Services conforming in all material respects to the specifications, functions, descriptions, standards, and criteria set forth in the Documentation; (c) that the Service Level Standards can be achieved; and (d) that the SaaS Software Services work with the non-hosted browser version.

The following provisions shall also apply, but only if the City provides Contractor with a written request so naming each section below upon issuance of the Agreement and accompanying Purchase Orders:

- i. **Planning:** Contractor must assist the City with the planning and logistics of upgrades and updates.
- ii. **Technical Assistance.** Contractor must provide technical assistance regarding release notes, new functionality, and new application workflows.
- iii. **Deployment:** Deployment of these revisions will be mutually agreed upon between Contractor and City.
- iv. **Software Releases:** Release of Software revisions as defined will be conducted on a schedule as determined by Contractor. Contractor shall provide no less than a thirty (30) calendar day prior written notice of when any such revision is scheduled to be released. City will be granted a fifteen (15) calendar day evaluation window to review release documentation regarding software modules being impacted and general revision changes.
- v. **Testing.** After the evaluation period, Contractor shall conduct a deployment of the revision to the City test environment. The Software deployment will be scheduled in writing five (5) calendar days prior to actual deployment activities. As part of the upgrade activities within the Test Environment, Contractor may provide nominal testing to ensure all systems are functional and the revision deployment was successful. Post deployment activities include an e-mail or portal post to serve as written notification that this service has been completed. City shall have forty-five (45) calendar day test window in which City has ability to test and raise issues with Contractor. Test environment deployment activities will be conducted during a mutually agreed-to time window and may not necessarily align with the production maintenance windows as described within this document.
- vi. **Severity 1 and Severity 2 Incident Correction:** If a SaaS Severity Level 1 or Severity Level 2 Issue is identified and appropriately triaged and classified by both Contractor and City during the test environment deployment test window, Contractor shall correct the SaaS Issue. The severity of a SaaS Issue will be initially defined by the City and confirmed by Contractor. Until the SaaS Issue has been resolved, the Severity Level may be raised or lowered based on Contractor's analysis of impact to business. If the SaaS Issue can be corrected and can be redeployed within the remainder of the deployment test window, City will have an

additional five (5) testing days in which to evaluate and further test for the SaaS Issue resolution. If the SaaS Issue cannot be corrected within the remainder of the test window, Contractor will deploy immediately upon availability with as much notice as practicable. City will be allowed an additional five (5) testing days to evaluate the correction post the test window if desired.

- vii. **Testing Suspension:** If at any time during the testing window City identifies the presence of multiple SaaS Severity Level 1 or Severity Level 2 Issues that can be shown to materially impact City ability to continue testing, City may in writing elect to suspend testing until corrections for the SaaS Issues can be provided. Contractor will deploy corrections immediately upon availability with as much notice as practicable. Upon release of corrections, City will have five (5) calendar days to commence the testing within the then available remaining testing window.
- viii. **Software Promotion:** Contractor will promote revision from Test Environment to Production and Back-up environments after the provided test window has elapsed. The Software promotion will be scheduled in writing five (5) calendar days prior to actual deployment activities. As part of the promotion activities within the Production and Back-up environment, Contractor may provide nominal testing to ensure all systems are functional and the revision promotion was successful. Post promotion activities include an e-mail or portal post to serve as written notification that this service has been completed. At the point of e-mail or portal posting, the new revision will be considered “in production” and supported under the maintenance service terms described here within.
- ix. **Documentation.** In support of such SaaS Software Version upgrades, SaaS Software Revisions and SaaS Software patches, Contractor shall provide updated user technical documentation reflecting the SaaS Software Version upgrades, SaaS Software Revisions and SaaS Software patches as soon as reasonably practical after the SaaS Software Version upgrades, SaaS Software Revisions and SaaS Software Patches have been released. Updated user technical documentation that corrects SaaS Software Errors or other minor discrepancies will be provided to Contractor’s customers when available.
- x. **Training.** Contractor must provide standard training using Contractor’s upgrade tools and provide ongoing knowledge transfer to the City.

2. **Third-Party Software Revisions.** At its election, Contractor will provide periodic software revisions of Third-Party Software with the SaaS Software without further charge provided the following conditions are met: (i) the Third-Party Software revision corrects a malfunction or significant publicly disclosed security threat in the Third-Party Software that affects the operation or ability to provide secure use of the SaaS Software; and (ii) the Third-Party Software Revision has, in the opinion of Contractor, corrected malfunctions or a significant security threat identified in Contractor's Technology System and has not created any additional malfunctions; and (iii) the Third-Party Software revision is available to Contractor. City is responsible for obtaining and installing or requesting installation of the Third-Party Software revision if the Third-Party Software was not licensed to City by or through Contractor. Contractor Software revisions provided by Contractor are specifically limited to the Third-Party Software identified and set forth in the Agreement and accompanying Purchase Orders.

C. Response to SaaS Issues. Contractor shall provide verbal or written responses to SaaS Issues identified by City in an expeditious manner. Such responses shall be provided in accordance with the Target Response Times defined under Section V of this Appendix (Technical Support).

D. SaaS Software Maintenance Acceptance Period. Unless otherwise agreed to by City on a case-by-case basis, for non-emergency maintenance, City shall have a twenty (20) business day period to test any maintenance changes prior to Contractor introducing such maintenance changes into production. If the City rejects, for good cause, any maintenance changes during the SaaS Software Maintenance Acceptance Period, Contractor shall not introduce such rejected maintenance changes into production. At the end of the Maintenance Acceptance Period, if City has not rejected the maintenance changes, the maintenance changes shall be deemed to be accepted by City and Contractor shall be entitled to introduce the maintenance changes into production.

E. SaaS Hardware: Contractor shall use commercially reasonable efforts to ensure that all hardware (including servers, routers, and other related equipment) on which the SaaS Application is deployed are attached to back-up power systems sufficient to maintain the site's availability for so long as any power outage could reasonably be expected to occur, based on the experience of Contractor at its deployment location and consistent with the Tier rating of the Data Center required under Section (I)(E) of this Appendix.

IV. City Responsibilities

A. City shall provide Contractor with timely notification of any SaaS Issues or SaaS Software Errors by either of these methods:

1. **Contacting Contractor's Customer Support;** or
2. **By entering the problem on Contractor's Service Portal;** or

B. Support for Problem Investigation. City shall support all reasonable requests by Contractor as may be required in problem investigation and resolution.

C. SaaS Incident Manager: Designation of Point of Contact. City shall assign an individual or individuals to serve as the designated contact(s) for all communication with Contractor during SaaS Issue investigation and resolution.

D. Discovery of SaaS Software Errors. Upon discovery of a SaaS Software Error, City agrees, if requested by Contractor, to submit to Contractor a listing of output and any other data that Contractor may require in order to reproduce the SaaS Software Error and the operating conditions under which the SaaS Software Error occurred or was discovered.

V. 24X7 Technical Support:

A. 24x7 Technical Support: Authorized Users will make Technical Support requests 24/7 by calling or emailing Contractor’s Technical Support staff or by submitting a request via Contractor’s service desk web portal. The Technical Support staff shall assign to the request the Incident Severity Level (as defined herein) indicated by the City. Severity Level 1 and 2 Incidents items will be addressed 24/7/365. Severity Level 3 and 4 Incidents will be addressed during the standard business hours of 6:00 a.m. - 6:00 p.m. US Pacific Time.

Incident Severity Level	Target Response Time
<p>Severity Level 1: Requires immediate attention – Critical production functionality is not available or a large number of users cannot access the SaaS Application. Causes a major business impact where service is lost or degraded and no workaround is available, preventing operation of the business.</p>	<p>Request Response Time: 15 minutes. Request Resolution Time Target: < 2 hours. Maximum Permitted Request Resolution Time: < 12 hours <i>City shall be entitled to a Service Credit of 15% of the Monthly Hosting Fee paid for each failure timely to achieve resolution. If Fees are paid annually, the 15% shall apply to 1/12 of that annual fee.</i></p>
<p>Severity Level 2: Requires priority attention – Some important production functionality is not available, or a small number of users cannot access the system. Causes significant business impact where service is lost or degraded and no workaround is available; however, the business can continue to operate in a limited fashion.</p>	<p>Request Response Time: 30 minutes Request Resolution Time Target: < 4 hours Maximum Permitted Request Resolution Time: < 48 hours <i>City shall be entitled to a Service Credit of 10% of the Monthly Hosting Fee paid for each failure timely to achieve resolution. If Fees are paid annually, the 10%</i></p>

Incident Severity Level	<i>Target Response Time</i>
	<i>shall apply to 1/12 of that annual fee.</i>
<p>Severity Level 3: Requires attention – There is a problem or inconvenience. Causes a business impact where there is minimal loss of service and a workaround is available such that the system can continue to operate fully and users are able to continue business operations.</p>	<p>Request Response Time: 1 hr. Request Resolution Time Target: < 8 hours Maximum Permitted Request Resolution Time: < 96 hours <i>City shall be entitled to a Service Credit of 5% of the Monthly Hosting Fee paid for each failure timely to achieve resolution. If Fees are paid annually, the 15% shall apply to 1/12 of that annual fee.</i></p>
<p>Severity Level 4: There is a problem or issue with no loss of service and no business impact.</p>	<p>Request Response Time: 4 hr. Request Resolution Time Target: < 96 hours Maximum Permitted Request Resolution Time: < 7 days</p>

1. SERVICE CREDIT ESCALATION.

In the event of a Severity Level 1 issue that is not resolved sufficiently quickly as determined in the City’s sole discretion, City may escalate the problem to Contractor's Chief Technology Officer.

2. ROOT CAUSE ANALYSIS

Following the resolution of a Severity Level 1 OR Level 2 incident, Contractor will discuss with City the cause of the failure, the actions Contractor took to resolve the failure, a timeline of the event and the actions Contractor plans to take to prevent such failure from recurring, and, if requested, Contractor will provide City a written summary of such discussion. Contractor will, on request, provide detailed documentation of the root cause analysis and preventative actions taken or planned with clear dates for completion of the action(s).

Appendix B

Service Level Obligations: Minimum Requirements

The following represent minimum requirements that Contractor shall meet or exceed with regards to its Service Level Obligations.

A. Time is of the Essence. For the term of the Term Sheet and the Agreement, Contractor shall provide SaaS Services, Force Majeure events excepted, during the applicable Service Windows and in accordance with the applicable Service Levels as described herein, time being of the essence.

B. Service Levels.

1. Availability Service Level:

a. Definitions:

- i. Actual Uptime:** The total minutes in the reporting month that the Services were actually available to Authorized Users for normal use.
- ii. Scheduled Downtime:** The total minutes in the reporting month during which Scheduled SaaS Maintenance was performed.
- iii. Scheduled Uptime:** The total minutes in the reporting month less the total minutes represented by the Scheduled Downtime.

b. Service Level Standard. Services shall be available to Authorized Users for normal use 100% of the Scheduled Uptime.

i. Calculation: $(\text{Actual Uptime} / \text{Scheduled Uptime}) * 100 = \text{Percentage Uptime}$ (as calculated by rounding to the second decimal point)

ii. Performance Credit.

- 1) Where Percentage Uptime is greater than 99.9%:** No Performance Credit will be due to City.
- 2) Where Percentage Uptime is equal to or less than 99.9%:** City shall be due a Performance Credit in the amount of 20% of the Services Fees (as calculated on a monthly basis for the reporting month) for each full 1% reduction in Percentage Uptime.

2. Response Time Service Level.

a. Definition(s).

- i. Response Time:** The interval of time from when an Authorized User requests, via the Services, a Transaction to when visual confirmation

of Transaction completion is received by the Authorized User. For example, Response Time includes the period of time representing the point at which an Authorized User enters and submits data to the Services and the Services display a message to the Authorized User that the data has been saved.

ii. Total Transactions: The total of Transactions occurring in the reporting month.

iii. Transaction(s): Services web page loads, Services web page displays, and Authorized User Services requests.

b. Service Level Standard. Transactions shall have a Response Time of two (2) seconds or less 99.9% of the time each reporting month during the periods for which the Services are available.

i. Calculation. $((\text{Total Transactions} - \text{Total Transactions failing Standard}) / \text{Total Transactions}) * 100 = \text{Percentage Response Time}$ (as calculated by rounding to the second decimal point).

ii. Performance Credit.

1) Where Percentage Response Time is greater than 99.9%: No Performance Credit will be due to City.

2) Where Percentage Response Time is equal to or less than 99%: City shall be due a Performance Credit in the amount of 20% of the Services Fees (as calculated on a monthly basis for the reporting month) for each full 1% reduction in Percentage Response Time.

3. Technical Support Problem Response Service Level.

a. Definition.

i. Total Problems: The total number of problems occurring in the reporting month.

b. Service Level Standard. Problems shall be confirmed as received by Contractor 100% of the time each reporting month, in accordance with the Request Response Time associated with the SaaS Severity Level.

i. Calculation. $((\text{Total Problems} - \text{Total Problems failing Standard}) / \text{Total Problems}) * 100 = \text{Percentage Problem Response}$ (as calculated by rounding to the second decimal point). Note: This Calculation must be completed for each SaaS Severity Level.

ii. Performance Credit.

1) SaaS Severity Level 1 – 2.

- i) Where Percentage Problem Response is greater than 99.9%:** No Performance Credit will be due to City.
- ii) Where Percentage Problem Response is equal to or less than 99%:** City shall be due a Performance Credit in the amount of 20% of the Services Fees (as calculated on a monthly basis for the reporting month) for each full 1% reduction in Percentage Problem Response.

2) SaaS Severity Level 3 – 4.

- i) Where Percentage Problem Response is greater than 99.9%:** No Performance Credit will be due to City.
- ii) Where Percentage Problem Response is equal to or less than 99%:** City shall be due a Performance Credit in the amount of 20% of the Services Fees (as calculated on a monthly basis for the reporting month) for each full 1% reduction in Percentage Problem Response.

C. Service Level Reporting. On a monthly basis, in arrears and no later than the fifteenth (15th) calendar day of the subsequent month following the reporting month, Contractor shall provide reports to City describing the performance of the SaaS Services and of Contractor as compared to the service level standards described herein. The reports shall be in a form agreed-to by City, and, in no case, contain no less than the following information: (a) actual performance compared to the Service Level Standard; (b) the cause or basis for not meeting the service level standards described herein; (c) the specific remedial actions Contractor has undertaken or will undertake to ensure that the service level standards described herein will be subsequently achieved; and (d) any Performance Credit due to City. Contractor and City will meet as often as shall be reasonably requested by City, but no less than monthly, to review the performance of Contractor as it relates to the service level standards described herein. Where Contractor fails to provide a report for a service level standard described herein in the applicable timeframe, the service level standard shall be deemed to be completely failed for the purposes of calculating a Performance Credit. Contractor shall, without charge, make City's historical service level standard reports to City upon request.

D. Failure to Meet Service Level Standards. In the event Contractor does not meet a service level standard described herein, Contractor shall: (a) owe to City any applicable Performance Credit, as liquidated damages and not as a penalty; and, (b) use its best efforts to ensure that any unmet service level standard described herein is subsequently met. Notwithstanding the foregoing, Contractor will use its best efforts to minimize the impact or

duration of any outage, interruption, or degradation of Service. In no case shall City be required to notify Contractor that a Performance Credit is due as a condition of payment of the same.

E. Termination for Material and Repeated Failures. City shall have, in addition to any other rights and remedies under the Term Sheet and the Agreement or at law, the right to immediately terminate the Term Sheet and the Agreement and be entitled to a return of any prepaid fees where Contractor fails to meet any service level standards described herein: (a) to such an extent that the City's ability, as solely determined by City, to use the SaaS Services is materially disrupted, Force Majeure events excepted; or, (b) for four (4) months out of any twelve (12) month period.

F. Audit of Service Levels. No more than quarterly, and upon written request by City upon issuance of the Agreement and accompanying Purchase Orders, City shall have the right to audit Contractor's books, records, and measurement and auditing tools to verify service level obligations achievement and to determine correct payment of any Performance Credit. Where it is determined that any Performance Credit was due to City but not paid, Contractor shall immediately owe to City the applicable Performance Credit.

Appendix C

Disaster Recovery Plan: Minimum Requirements

The following represent minimum requirements that Contractor shall meet or exceed with regard to its Disaster Recovery Plan.

- A.** In the case of emergency or failure, this Disaster Recovery plan will be used to restore and continue service. Disaster Recovery is required when Contractor, in good faith, feels that an emergency failure jeopardizes its ability to meet its Service Level Obligations. Contractor shall use best efforts to restore operations at the same location or, at Contractor's discretion, a backup location. City acknowledges and agrees that such an event may result in partial or degraded service when restored. The pre-disaster/loss level of service shall be restored as soon as commercially reasonable.

- B. Restoration Targets:** Restoration of services timeframes will be defined and measured as Recovery Point Objectives and Recovery Time Objectives.

- C. Recovery Point Objective:** The Recovery Point Objective (RPO) is defined to be the maximum acceptable amount of data loss for which City may experience due to a temporary loss of hosted services and applications. Contractor shall deliver a maximum RPO of eight (8) hours based on incremental backups being made available between production and backup facilities and recovery, if any, of production data.

- D. The Recovery Time Objective:** The Recovery Time Objective (RTO) is the maximum period of continuous time during which access to the SaaS Application shall not be available to the City. Contractor shall deliver a maximum RTO of forty-eight (48) hours for the SaaS Application.

- E. Data Synchronization:** Data Synchronization is the act of replicating or "mirroring" data from the Primary Environment to an off-site "backup" location (the Back-up Tier 2 Data Center). Data Synchronization is to be used in the case of a Disaster Recovery event to restore service. Data Synchronization must occur at a set interval of once per eight (8) hours for incremental data set changes and weekly for a full backup.

- F. Recovery Testing:** Contractor shall regularly test and exercise the Disaster Recovery Plan to ensure that the Tier 2 Back-up Data Center and Data Synchronization processes are functioning as expected. City shall allow for a maximum of a two (2) week runtime within the Back-Up Data Center before returning system operation to Primary Data Center.

- G. Backup and Recovery:** Backups of the production servers will occur every 8 hours, retained for thirty (30) days, and stored locally at the primary data center on a separate managed storage device. These images will be used to recover servers if any issues occur. The backup images will periodically be replicated throughout the day to the secondary staged server environment for the purposes of site recovery. This replication will occur on a private protected fiber ring connecting the two data centers. In the event of a site disaster, a request

can be made to the support desk and the most current server image set can be brought up as the production environment.