

AGREEMENT FOR PROFESSIONAL SERVICES

This is an Agreement between the City of Berkeley, a Charter City organized and existing under the laws of the State of California ("City"), and _____ ("Provider"), a California [corporation, partnership, joint venture], doing business at _____ who agree as follows:

RECITALS

WHEREAS, this Agreement sets forth the terms and conditions under which City shall obtain and Provider will provide the services identified in Appendix "A" attached hereto;

Now, THEREFORE, City and Provider agree as follows:

1. DEFINITIONS

- 1.1 Where any word or phrase defined below, or a pronoun in place thereof, is used in any part of this Agreement, it shall have the meaning herein set forth.
 - 1.1.1 Agreement: This Agreement together with all attachments and appendices and other documents incorporated herein by reference.
 - 1.1.2 Project: Total design of _____ of which the Work performed under this Agreement may be whole or part.
 - 1.1.3 Project Manager: Person or persons designated by City and authorized to act on City's behalf with respect to this Agreement.
 - 1.1.4 Work: The work described in Appendix A "Scope of Services", and made a part of this Agreement.

2. TERM OF THIS AGREEMENT

- 2.1 This Agreement shall begin on _____ and end on _____. The City Manager of the City or his/her designee may extend the term of this Agreement by giving written notice.

3. SERVICES PROVIDER AGREES TO PERFORM

Provider agrees to perform the services provided for in Appendix "A", as authorized from time to time by City in writing, in the manner provided in this Agreement. Time is of the essence in the performance of this Agreement.

4. COMPENSATION

- 4.1 Compensation shall be due Provider according to the Compensation Schedule established in Appendix "B", "Compensation for Services," in a total amount not to exceed \$ _____. Provider shall invoice its time at its ordinary billing rates.
- 4.2 City will not withhold the entire payment if a questioned amount is involved, but will issue payment in the amount of the total invoice less any questioned amount. Payment for questioned amount(s) will be made upon City's receipt of any requested documentation verifying the questioned amount(s) and City's determination that the questioned amount(s) is reimbursable under the terms of this Agreement.
- 4.3 Invoices furnished by Provider under this Agreement must be in a form acceptable to City. All amounts paid by City to Provider shall be subject to audit by City. Payment shall be made by City to Provider at the address stated in Appendix "A".

5. QUALIFIED PERSONNEL; NO SUBCONSULTING

- 5.1 Work under this Agreement shall be performed only by competent personnel under the supervision of and in the employment of Provider. Provider will conform with City's reasonable requests regarding assignment of personnel, but all personnel, including those assigned at City's request, shall be supervised by Provider.
- 5.2 Provider agrees that any personnel referred to in Appendix "A" will continue their assignments on the Project during the entire term of this Agreement, as described in Appendix "A."
- 5.3 Provider is prohibited from subcontracting this Agreement or any part of it unless such subcontracting is approved by City in writing. Neither party shall, on the basis of this Agreement, contract on behalf of or in the name of the other party. An agreement made in violation of this provision shall confer no rights on any party and shall be null and void.
- 5.4 City retains the right to approve any replacement staff should Provider staff become unavailable to work on this project due to resignation, termination or promotion.

6. REPRESENTATIONS

- 6.1 Provider represents that it is qualified to perform the Work and that it possesses the necessary licenses and/or permits required to perform the Work or will obtain such licenses and/or permits prior to time such licenses and/or permits are required.
- 6.2 Provider represents that the Work shall be performed in a professional manner and shall conform to the standards of practice observed on similar, successfully completed projects by specialists in the Work to be provided. Provider agrees that, if the Work is not so performed, in addition to all of its obligations under this Agreement and at law, Provider shall reperform or replace unsatisfactory Work at no additional expense to City.
- 6.3 The granting of any progress payment by City, or the receipt thereof by Provider, or any inspection, review, approval or oral statement by any representative of City, or State certification, shall in no way waive or limit the certification obligations in this Paragraph or lessen the liability of Provider to reperform or replace unsatisfactory Work, including but not limited to cases where the unsatisfactory character of such work may not have been apparent or detected at the time of such payment, inspection, review or approval.
- 6.4 Nothing in this Paragraph shall constitute a waiver or limitation of any right or remedy, whether in equity or at law, which City or Provider may have under this Agreement or any applicable law. All rights and remedies of City, whether under this Agreement or other applicable law, shall be cumulative.

7. INDEMNIFICATION BY PROVIDER

- 7.1 General Liability. To the fullest extent permitted by law (including, without limitation, California Civil Code Sections 2782 and 2782.8), Provider shall indemnify, defend and save harmless City from and against any and all claims, losses, costs, damages and expenses resulting from property damage, bodily injury or death (including reimbursement of reasonable attorneys' fees), to the extent arising out of the operations of Provider, its subProviders or anyone employed by them.
- 7.2 Professional Liability. Notwithstanding the foregoing or any other term(s) in this or any other agreement, with respect to Provider's professional liability (as opposed to Provider's operations covered by Commercial General Liability Insurance), to the fullest extent permitted by law (including, without limitation, California Civil Code Sections 2782 and 2782.8), Provider shall indemnify and hold harmless City from any and all losses, costs, damages and expenses, (including the reimbursement of reasonable attorneys' fees), that arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of the Provider. In no event shall the cost to defend charged to Provider exceed the Provider's proportionate percentage of fault.

8. LIABILITY OF CITY

8.1 Notwithstanding any other provision of this Agreement, in no event shall City be liable, regardless of whether any claim is based on contract or tort, for any special, consequential, indirect or incidental damages, including, but not limited to, lost profits or revenue, arising out of or in connection with this Agreement or the services performed in connection with this Agreement.

9. INDEPENDENT CONTRACTOR; PAYMENT OF TAXES AND OTHER EXPENSES

9.1 Provider shall be deemed at all times to be an independent contractor and shall be wholly responsible for the manner in which Provider performs the services required of Provider by the terms of this Agreement. Provider shall be liable for its acts and omissions, and those of its employees and its agents. Nothing contained herein shall be construed as creating an employment, agency or partnership relationship between City and Provider.

9.2 Terms in this Agreement referring to direction from City shall be construed as providing for direction as to policy and the result of Provider's Work only and not as to the means or methods by which such a result is obtained.

9.3 Except as expressly provided in this Agreement, nothing in this Agreement shall operate to confer rights or benefits on persons or entities not party to this Agreement.

9.4 Payment of any taxes, including California Sales and use Taxes, levied upon this Agreement, the transaction, or the services or goods delivered pursuant hereto, shall be the obligation of Provider.

10. INSURANCE

10.1 Prior to the execution of this Agreement, Provider shall furnish to City satisfactory proof that Provider has taken out for the entire period covered by this Agreement, as further defined below, the following insurance in a form satisfactory to City and with an insurance carrier satisfactory to City, authorized to do business in California and rated by A. M. Best & Company A minus or better, financial category size seven (7) or better, which will protect those described below from claims described below which arise or are alleged to have arisen out of or result from the services of Provider for which Provider may be legally liable, whether performed by Provider, or by those employed directly or indirectly by it, or by anyone for whose acts Provider may be liable:

10.1.1 Commercial general liability insurance, written on an "occurrence" basis, which shall provide coverage for bodily injury, death and property damage resulting from operations, products liability, blasting, explosion, collapse of buildings or structures, damage to underground structures and utilities, liability for slander, false arrest and invasion of privacy arising out of construction management operations, blanket contractual liability, broad form endorsement, a construction management endorsement, products and completed operations, personal and advertising liability, with per location limits of not less than \$2,000,000 general aggregate and \$2,000,000 each occurrence, subject to a deductible of not more than \$25,000 payable by Provider.

10.1.2 Business automobile liability insurance with limits not less than \$1,000,000 each occurrence including coverage for owned, non-owned and hired vehicles, subject to a deductible of not more than \$10,000 payable by Provider.

10.1.3 Full workers' compensation insurance for all persons whom Provider may employ in carrying out Work contemplated under Contract, in accordance with Act of Legislature of State of California, known as "Workers' Compensation Insurance and Safety Act", approved May 26, 1913, and all Acts amendatory or supplemental thereto. Workers' compensation policy shall include Employer Liability Insurance with limits not less than \$1,000,000 each accident.

10.1.4 Professional Liability Insurance, specific to this Project only, with limits not less than \$2,000,000 each claim with respect to negligent acts, errors or omissions in connection with

professional services to be provided under this Agreement, and any deductible not to exceed \$50,000 each claim, with no exclusion for claims of one insured against another insured.

- 10.1.5 **Technology Professional Liability Errors and Omissions Insurance** appropriate to the Provider's profession and work hereunder, with limits not less than \$2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Provider in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, copyright, trademark, invasion of privacy violations, information theft, release of private information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.
- 10.1.6 The Policy shall include, or be endorsed to include, property damage liability coverage for damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the City in the care, custody, or control of the Provider. If not covered under the Provider's liability policy, such "property" coverage of the Agency may be endorsed onto the Provider's Cyber Liability Policy as covered property as follows:
- 10.1.7 Cyber Liability coverage in an amount sufficient to cover the full replacement value of damage to, alteration of, loss of, or destruction of electronic data and/or information "property" of the City that will be in the care, custody, or control of Provider.
- 10.2 Insurance policies shall contain an endorsement containing the following terms:
 - 10.2.1 City, and its directors, officers, partners, representatives, employees, Providers, subProviders and agents, shall be named as additional insureds, but only with respect to liability arising out of the activities of the named insured, and there shall be a waiver of subrogation as to each named and additional insured.
 - 10.2.2 The policies shall apply separately to each insured against whom claim is made or suit is brought except with respect to the limits of the company's liability.
 - 10.2.3 Written notice of cancellation, non-renewal or of any material change in the policies shall be mailed to City thirty (30) days in advance of the effective date thereof.
 - 10.2.4 Insurance shall be primary insurance and no other insurance or self insured retention carried or held by any named or additional insureds other than the Provider shall be called upon to contribute to a loss covered by insurance for the named insured.
- 10.3 Certificates of Insurance and Endorsements shall have clearly typed thereon the title of the Contract, shall clearly describe the coverage and shall contain a provision requiring the giving of written notice described above in subparagraph 10.2.3.
- 10.4 At the time of making an application for an extension of time, Provider shall submit evidence that insurance policies will be in effect during requested additional period of time.
- 10.5 Nothing herein contained shall be construed as limiting in any way the extent to which Provider or any of its permitted subcontractors or subProviders may be held responsible for payment of damages resulting from their operations.
- 10.6 If Provider fails to maintain any required insurance, City may take out such insurance, and deduct and retain amount of premium from any sums due Provider under this Agreement.
- 10.7 Provider shall forward all insurance documents to Kalai Chu, Senior Management Analyst, Department of Information Technology, 2180 Milvia Street, 4th Floor, Berkeley, CA 94704.

11. SUSPENSION OF WORK

City may, without cause, order Provider, in writing, to suspend, delay or interrupt Work pursuant to this Agreement, in whole or in part, for such periods of time as City may determine, in its sole discretion. Suspension shall be effected by delivery to Provider of a written notice of suspension specifying the extent to which performance of the Work under this Agreement is suspended, and the date upon which the suspension becomes effective, which shall be no less than seven (7) calendar days from the date the notice of suspension is delivered. Suspension of Work shall be treated as an excusable delay.

12. TERMINATION OF AGREEMENT FOR CAUSE

12.1 If at any time City believes Provider may not be adequately performing its obligations under this Agreement or may fail to complete the Work as required by this Agreement, City may request from Provider written assurances of performance and a written plan to correct observed deficiencies in Provider's performance if written notice of the same is provided by City. Failure to provide written assurances constitutes grounds to declare a default under this Agreement.

12.2 Provider shall be in default of this Agreement and City may, in addition to any other legal or equitable remedies available to City, terminate Provider's right to proceed under the Agreement, for cause, should Provider commit a breach of this Agreement and not cure such breach within ten (10) calendar days of the date of notice from City to Provider demanding such cure; or, if such failure is curable but not curable within such ten (10) day period, within such period of time as is reasonably necessary to accomplish such cure. (In order for Provider to avail itself of this time period in excess of 10 calendar days, Provider must provide City within the 10 day period a written plan acceptable to City to cure said breach, and then diligently commence and continue such cure according to the written plan.)

12.3 In the event a termination for cause is determined to have been made wrongfully or without cause, then the termination shall be treated as a termination for convenience, and Provider shall have no greater rights than it would have had if a termination for convenience had been effected in the first instance. No other loss, cost, damage, expense or liability may be claimed, requested or recovered.

13. TERMINATION OF AGREEMENT FOR CONVENIENCE

13.1 City may terminate performance of the Work under the Agreement in accordance with this Paragraph in whole, or from time to time in part, whenever City shall determine that termination is in the best interest of City. Termination shall be effected by delivery to Provider of notice of termination specifying the extent to which performance of the Work under the Agreement is terminated, and the date upon which termination becomes effective, which shall be no less than twenty-one (21) calendar days from the date the notice of termination is delivered. Provider shall then be entitled to recover its costs expended up to that point plus a reasonable profit, but no other loss, cost, damage, expense or liability may be claimed, requested or recovered.

13.2 Except as provided in this Agreement, in no event shall City be liable for costs incurred by or on behalf of Provider after the effective date of a notice of termination.

13.3 Termination under this provision shall not be construed as a waiver of any right or remedy otherwise available to City.

14. PROPRIETARY OR CONFIDENTIAL INFORMATION OF CITY

Provider understands and agrees that, in the performance of the services under this Agreement or in the contemplation thereof, Provider may have access to private or confidential information that may be owned or controlled by City and that such information may contain proprietary or confidential details, the disclosure of which to third parties may be damaging to City. Provider agrees that all information disclosed by City to Provider shall be held in confidence and used only in performance of the Agreement. Provider shall exercise the same standard of care to protect such information as a reasonably prudent Provider would use to protect its own proprietary data.

15. NOTICES TO THE PARTIES

All notices to be given by the parties hereto shall be in writing and effective when served by depositing same in the United States Post Office, postage prepaid and addressed as follows:

To City:

City of Berkeley
2180 Milvia St. Fourth Floor
Berkeley, CA 94704
Attn: Director of Information Technology

To Provider:

16. OWNERSHIP OF RESULTS/WORKS FOR HIRE

- 16.1 When this Agreement is terminated, Provider agrees to return to City all documents, drawings, photographs and other written or graphic material, however produced, that it received from City, its contractors or agents, in connection with the performance of its services under this Agreement. All materials shall be returned in the same condition as received.
- 16.2 Any interest of Provider or its subcontractors or subProviders, in studies, reports, memoranda, computational sheets or other documents prepared by Provider or its subcontractors or subProviders in connection with services to be performed under this Agreement shall become the property of City. Provider may, however, retain one copy for its files.
- 16.3 Any and all work, artwork, copy, posters, billboards, photographs, videotapes, audiotapes, systems designs, software, reports, designs, specifications, drawings, diagrams, surveys, source codes or any original works of authorship created by Provider or its subcontractors or subProviders in connection with services performed under this Agreement shall be works for hire as defined under Title 17 of the United States Code, and all copyrights in such works are the property of City. In the event that it is ever determined that any such works created by Provider or its subcontractors or subProviders under this Agreement are not works for hire under U.S. law, Provider hereby assigns all copyrights to such works to City. With the prior written approval of City's Project Manager, Provider may retain and use copies of such works for reference and as documentation of its experience and capabilities.

17. AUDIT AND INSPECTION OF RECORDS

- 17.1 Provider shall maintain all drawings, specifications, calculations, cost estimates, quantity takeoffs, statements of costs and completion dates, schedules and all correspondence, internal memoranda, papers, writings, and documents of any sort prepared by or furnished to Provider during the course of performing the Work and providing services with respect to the Project, for a period of at least three (3) years following final completion and acceptance of the Project, except that all such items pertaining to hazardous materials shall be maintained for at least thirty (30) years. All such records shall be available to City upon request at reasonable times and places. Monthly records of Provider's personnel costs, Provider costs, and reimbursable expenses shall be kept on a generally recognized accounting basis, and shall be available to City upon request at reasonable times and places. Provider shall not destroy any Project records until after advising City and allowing City to accept and store the records.
- 17.2 Provider agrees to maintain and make available to City during business hours accurate books and accounting records relative to its activities under this Agreement. Provider shall permit City to audit, examine and make copies, excerpts and transcripts from such books and records, and to make audits of all invoices, materials, payrolls, records or personnel and other data related to all other matters covered by this Agreement, whether funded in whole or in part under this Agreement. Provider shall maintain such data and records in an accessible location and condition for a period of not less than five years after final payment under this Agreement or until after final audit has been resolved, whichever is later. The

State of California or any federal agency having an interest in the subject of this Agreement shall have the same rights conferred upon City by this Paragraph.

- 17.3 The rights and obligations established pursuant to this Paragraph shall be specifically enforceable and survive termination of this Agreement.

18. DISPUTES

18.1 Should any question arise as to the meaning and intent of this Agreement, the question shall, prior to any other action or resort to any other legal remedy, be referred to the City's Project Manager and a principal of the Provider who shall decide the true meaning and intent of the Agreement. Such referral may be initiated by written request from either party and a meeting between the City's Project Manager and principal of the Provider shall take place within five days of the request.

18.2 Provider shall continue its Work throughout the course of any and all disputes, and Provider's failure to continue work during any and all disputes shall be considered a material breach of this Agreement, provided City continues to make payment to Provider for undisputed work completed by Provider. Provider further agrees that should Provider stop work due to a dispute or disputes, any and all claims, whether in law or in equity Provider may have against City, their officers, agents, representatives, and employees, whether such claims are pending, anticipated or otherwise, shall be deemed to have been waived and forever barred.

19. AGREEMENT MADE IN CALIFORNIA/VENUE

19.1 This Agreement shall be deemed to have been executed in Alameda County. The formation, interpretation and performance of this Agreement shall be governed by the laws of the State of California, excluding its conflict of laws rules. Venue for all litigation relative to the formation, interpretation and performance of this Agreement shall be in Alameda County, California.

19.2 This Agreement shall be executed in duplicate. One duplicate original shall be retained by City and one duplicate original shall be given to Provider.

20. CONFORMITY WITH LAW AND SAFETY

20.1 Provider shall observe and comply with all applicable laws, ordinances, codes and regulations of governmental agencies, including federal, state, municipal and local governing bodies having jurisdiction over any or all of the scope of services, including all provisions of the Occupational Safety and Health Act of 1979 as amended, all California Occupational Safety and Health Regulations, the California Building Code, the American with Disabilities Act, any copyright, patent or trademark law and all other applicable federal, state, municipal and local safety regulations. All services performed by Provider must be in accordance with these laws, ordinances, codes and regulations. Provider's failure to comply with any laws, ordinances, codes or regulations applicable to the performance of the work hereunder shall constitute a breach of contract.

20.2 If a death, serious personal injury or substantial property damage occurs in connection with the performance of this Contract, Provider shall immediately notify the City's Risk Manager by telephone. If any accident occurs in connection with this Contract, Provider shall promptly submit a written report to City, in such form as the City may require. This report shall include the following information: 1) name and address of the injured or deceased person(s); 2) name and address of Provider's subcontractor or subProvider, if any; 3) name and address of Provider's liability insurance carrier; and 4) a detailed description of the accident, including whether any of City's equipment, tools or materials were involved.

20.3 If a release of hazardous materials or hazardous waste that cannot be controlled occurs in connection with the performance of this Contract, Provider shall immediately notify the Berkeley Police Department and the City's Health Protection office.

20.4 Provider shall not store hazardous materials or hazardous waste within the City of Berkeley without a proper permit from the City.

21. SAFETY DATA SHEETS

- 21.1 To comply with the City's Hazardous Communication Program, Provider agrees to submit Safety Data Sheets (SDS) for all "hazardous substances" Provider intends to use in the performance of work under this Contract in any City facility. "Hazardous substances" are defined as those substances so designated by the Director of Industrial Relations pursuant to the Hazardous Substances Information and Training Act (Labor Code sec. 6360 *et seq.*). The SDS for all products must be submitted to the City before commencing work. The SDS for a particular product must be reviewed and approved by the City's Risk Manager before Provider may use that product.
- 21.2 City will inform Provider about hazardous substances to which it may be exposed while on the job site and protective measures that can be taken to reduce the possibility of exposure.

22. NON-DISCRIMINATION

Provider hereby agrees to comply with the provisions of Berkeley Municipal Code ("B.M.C.") Chapter 13.26 as amended from time to time. In the performance of this Contract, Provider agrees as follows:

- 22.1 Provider shall not discriminate against any employee or applicant for employment because of race, color, religion, ancestry, national origin, age (over 40), sex, pregnancy, marital status, disability, sexual orientation or AIDS.
- 22.2 Provider shall permit the City access to records of employment, employment advertisements, application forms, EEO-1 forms, affirmative action plans and any other documents which, in the opinion of the City, are necessary to monitor compliance with this non-discrimination provision. In addition, Provider shall fill-out, in a timely fashion, forms supplied by the City to monitor this non-discrimination provision.

23. CONFLICT OF INTEREST PROHIBITED

- 23.1 In accordance with Government Code section 1090, Berkeley City Charter section 36 and B.M.C. Chapter 3.64, neither Provider nor any employee, officer, director, partner or member of Provider, or immediate family member of any of the preceding, shall have served as an elected officer, an employee, or a City board, committee or commission member, who has directly or indirectly influenced the making of this Contract.
- 23.2 In accordance with Government Code section 1090 and the Political Reform Act, Government Code section 87100 *et seq.*, no person who is a director, officer, partner, trustee, employee or Provider of the Provider, or immediate family member of any of the preceding, shall make or participate in a decision made by the City or a City board, commission or committee, if it is reasonably foreseeable that the decision will have a material effect on any source of income, investment or interest in real property of that person or Provider.
- 23.3 Interpretation of this section shall be governed by the definitions and provisions used in the Political Reform Act, Government Code section 87100 *et seq.*, its implementing regulations, manuals and codes, Government Code section 1090, Berkeley City Charter section 36 and B.M.C. Chapter 3.64.

24. NUCLEAR FREE BERKELEY

Provider agrees to comply with B.M.C. Chapter 12.90, the Nuclear Free Berkeley Act, as amended from time to time.

25. OPPRESSIVE STATES CONTRACTING PROHIBITION

- 25.1 In accordance with Resolution No. 59,853-N.S., Provider certifies that it has no contractual relations with, and agrees during the term of this Contract to forego contractual relations to provide personal services to, the following entities:
- (1) The governing regime in any Oppressive State.
 - (2) Any business or corporation organized under the authority of the governing regime of any Oppressive State.
 - (3) Any individual, firm, partnership, corporation, association, or any other commercial organization, including parent-entities and wholly-owned subsidiaries (to the extent that their operations are related to the purpose of its contract with the City), for the express purpose of assisting in business operations or trading with any public or private entity located in any Oppressive State.
- 25.2 Appendix A to Resolution No. 59,853-N.S. designates the following as Oppressive States for the purposes of this contract: Tibet Autonomous Region and the provinces of Adu, Kham, and U-Tsang.
- 25.3 Provider's failure to comply with this section shall constitute a default of this Contract and City may terminate this Contract pursuant to Section 12. In the event that the City terminates Provider due to a default under this provision, City may deem Provider a non-responsible bidder for five (5) years from the date this Contract is terminated.

26. SANCTUARY CITY CONTRACTING

Contractor hereby agrees to comply with the provisions of the Sanctuary City Contracting Ordinance, B.M.C. Chapter 13.105. In accordance with this Chapter, Contractor agrees not to provide the U.S. Immigration and Customs Enforcement Division of the United States Department of Homeland Security with any Data Broker or Extreme Vetting Services as defined herein:

- a. "Data Broker" means either of the following:
 - i. The collection of information, including personal information about consumers, from a wide variety of sources for the purposes of reselling such information to their customers, which include both private-sector business and government agencies;
 - ii. The aggregation of data that was collected for another purpose from that for which it is ultimately used.
- b. "Extreme Vetting" means data mining, threat modeling, predictive risk analysis, or other similar services. Extreme Vetting does not include:
 - i. The City's computer-network health and performance tools;
 - ii. Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, monitor for, prevent, and protect technology infrastructure and systems owned and operated by the City of Berkeley from potential cybersecurity events and cyber-forensic based investigations and prosecutions of illegal computer based activity.

27. RECYCLED PAPER FOR WRITTEN REPORTS

If Provider is required by this Contract to prepare a written report or study, Provider shall use recycled paper for said report or study when such paper is available at a cost of not more than ten percent more than the cost of virgin paper, and when such paper is available at the time it is needed. For the purposes of this Contract, recycled paper is paper that contains at least 50% recycled product. If recycled paper is not available, Provider shall use

white paper. Written reports or studies prepared under this Contract shall be printed on both sides of the paper whenever practical.

28. BERKELEY LIVING WAGE ORDINANCE

- 28.1 Provider hereby agrees to comply with the provisions of the Berkeley Living Wage Ordinance, B.M.C. Chapter 13.27. If Provider is currently subject to the Berkeley Living Wage Ordinance, as indicated by the Living Wage Certification form, attached hereto, Provider will be required to provide all eligible employees with City mandated minimum compensation during the term of this Contract, as defined in B.M.C. Chapter 13.27, as well as comply with the terms enumerated herein. Provider expressly acknowledges that, even if Provider is not currently subject to the Living Wage Ordinance, cumulative contracts with City may subject Provider to the requirements under B.M.C. Chapter 13.27 in subsequent contracts.
- 28.2 If Provider is currently subject to the Berkeley Living Wage Ordinance, Provider shall be required to maintain monthly records of those employees providing service under the Contract. These records shall include the total number of hours worked, the number of hours spent providing service under this Contract, the hourly rate paid, and the amount paid by Provider for health benefits, if any, for each of its employees providing services under the Contract. Provider agrees to supply City with any records it deems necessary to determine compliance with this provision. These records are expressly subject to the auditing terms described in Section 17.
- 28.3 If Provider is currently subject to the Berkeley Living Wage Ordinance, Provider shall include the requirements thereof, as defined in B.M.C. Chapter 13.27, in any and all subcontracts in which Provider engages to execute its responsibilities under this Contract. All subcontractor or subProvider employees who spend 25% or more of their compensated time engaged in work directly related to this Contract shall be entitled to a living wage, as described in B.M.C. Chapter 13.27 and herein.
- 28.4 If Provider fails to comply with the requirements of this Section, the City shall have the rights and remedies described in this Section, in addition to any rights and remedies provided by law or equity.
- 28.5 Provider's failure to comply with this Section shall constitute a material breach of the Contract, upon which City may terminate this Contract pursuant to Section 12. In the event that City terminates Provider due to a default under this provision, City may deem Provider a non-responsible bidder for not more than five (5) years from the date this Contract is terminated.

In addition, at City's sole discretion, Provider may be responsible for liquidated damage in the amount of \$50 per employee per day for each and every instance of an underpayment to an employee. It is mutually understood and agreed that Provider's failure to pay any of its eligible employees at least the applicable living wage rate will result in damages being sustained by the City; that the nature and amount of the damages will be extremely difficult and impractical to fix; that the liquidated damage set forth herein is the nearest and most exact measure of damage for such breach that can be fixed at this time; and that the liquidated damage amount is not intended as a penalty of forfeiture for Provider's breach. City may deduct any assessed liquidated damages from any payments otherwise due Provider.

29. BERKELEY EQUAL BENEFITS ORDINANCE

- 29.1 Provider hereby agrees to comply with the provisions of the Berkeley Equal Benefits Ordinance, B.M.C. Chapter 13.29. If Provider is currently subject to the Berkeley Equal Benefits Ordinance, as indicated by the Equal Benefits Certification form, attached hereto, Provider will be required to provide all eligible

employees with City mandated equal benefits, as defined in B.M.C. Chapter 13.29, during the term of this contract, as well as comply with the terms enumerated herein.

- 29.2 If Provider is currently or becomes subject to the Berkeley Equal Benefits Ordinance, Provider agrees to provide the City with all records the City deems necessary to determine compliance with this provision. These records are expressly subject to the auditing terms described in Section 17 of this contract.
- 29.3 If Provider fails to comply with the requirements of this Section, City shall have the rights and remedies described in this Section, in addition to any rights and remedies provided by law or equity.
- 29.4 Provider's failure to comply with this Section shall constitute a material breach of the Contract, upon which City may terminate this contract pursuant to Sections 12. In the event the City terminates this contract due to a default by Provider under this provision, the City may deem Provider a non-responsible bidder for not more than five (5) years from the date this Contract is terminated.

In addition, at City's sole discretion, Provider may be responsible for liquidated damages in the amount of \$50.00 per employee per day for each and every instance of violation of this Section. It is mutually understood and agreed that Provider's failure to provide its employees with equal benefits will result in damages being sustained by City; that the nature and amount of these damages will be extremely difficult and impractical to fix; that the liquidated damages set forth herein is the nearest and most exact measure of damages for such breach that can be fixed at this time; and that the liquidated damage amount is not intended as a penalty or forfeiture for Provider's breach. City may deduct any assessed liquidated damages from any payments otherwise due Provider.

30. PREVAILING WAGES

Certain labor categories under this contract may be subject to prevailing wages as identified in the State of California Labor Code commencing with Sections 1720 et. seq. and 1770 et. seq. These labor categories, when employed for any "work performed during the design and preconstruction phases of construction including, but not limited to, inspection and land surveying work," constitute a "Public Work" within the definition of Section 1720(a)(1) of the California Labor Code requiring payment of prevailing wages. In performing its obligations under this contract, Provider is solely responsible to determine which, if any, of the work is governed by a labor category pursuant to California Labor Code sections 1720 et. seq. and 1770 et. seq. and pay the pertinent prevailing wage. Provider shall defend, indemnify and hold harmless City concerning any liability arising out of Labor Code section 1720 et. seq. and 1770 et. seq.

31. SETOFF AGAINST DEBTS

Provider agrees that City may deduct from any payments due to Provider under this Contract any monies that Provider owes City under any ordinance, contract or resolution for any unpaid taxes, fees, licenses, unpaid checks or other amounts.

32. PROVIDERS TO SUBMIT STATEMENTS OF ECONOMIC INTEREST

The City's Conflict of Interest Code, Resolution No. 60,788-N.S., as amended, requires Providers who make a governmental decision or act in a staff capacity as defined in 2 Cal. Code of Regs. § 18700, as amended from time to time, to disclose conflicts of interest by filing a Statement of Economic Interest (Form 700). Providers agree to file such statements with the City Clerk at the beginning of the contract period and upon termination of the Provider's service.

33. CITY BUSINESS LICENSE, PAYMENT OF TAXES, TAX I.D. NUMBER

Provider has obtained a City business license as required by B.M.C. Chapter 9.04, and its license number is

written below; or, Provider is exempt from the provisions of B.M.C. Chapter 9.04 and has written below the specific B.M.C. section under which it is exempt. Provider shall pay all state and federal income taxes and any other taxes due. **Provider certifies under penalty of perjury that the taxpayer identification number written below is correct.**

34. MISCELLANEOUS

- 34.1 The Agreement, and any written modification to the Agreement, shall represent the entire and integrated Agreement between the parties hereto regarding the subject matter of this Agreement and shall constitute the exclusive statement of the terms of the parties' Agreement. The Agreement, and any written modification to the Agreement, shall supersede any and all prior negotiations, representations or agreements, either written or oral, express or implied, that relate in any way to the subject matter of this Agreement or written modification, and the parties represent and agree that they are entering into this Agreement and any subsequent written modification in sole reliance upon the information set forth in the Agreement or written modification and the parties are not and will not rely on any other information.
- 34.2 Either party's waiver of any breach, or the omission or failure of either party, at any time, to enforce any right reserved to it, or to require performance of any of the terms, covenants, conditions or other provisions of this Agreement, including the timing of any such performance, shall not be a waiver of any other right to which any party is entitled, and shall not in any way affect, limit, modify or waive that party's right thereafter to enforce or compel strict compliance with every term, covenant, condition or other provision hereof, any course of dealing or custom of the trade or oral representations notwithstanding. This Agreement may not be modified, nor may compliance with any of its terms be waived, except by written instrument executed and approved by fully authorized representatives of City and the Provider.
- 34.3 As between the parties to this Agreement: as to all acts or failures to act by either party to this Agreement, any applicable statute of limitations shall commence to run on the date of issuance by City's Project Manager of the final Certificate for Payment, or termination of this Agreement, whichever is earlier, except for latent defects, for which the statute of limitation shall begin running upon discovery of the defect and its cause.
- 34.4 Any provisions or portions thereof of this Agreement prohibited by, or made unlawful or unenforceable under any applicable law of any jurisdiction, shall as to such jurisdiction be ineffective without affecting other provisions or portions thereof of this Agreement. If the provisions of such applicable law may be waived, they are hereby waived to the end that this Agreement may be deemed to be a valid and binding agreement enforceable in accordance with its terms. If any provisions or portion thereof of this Agreement are prohibited by, or made unlawful or unenforceable under any applicable law and are therefore stricken or deemed waived, the remainder of this Agreement shall be interpreted to achieve the goals or intent of the stricken or waived provisions or portions thereof to the extent such interpretation is consistent with applicable law.

35. SEVERABILITY

- 35.1 If any part of this Agreement or the application thereof is declared invalid for any reason, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision or application, and to this end the provisions of this Agreement are declared to be severable.

36. ORDER OF PRECEDENCE OF DOCUMENTS

- 36.1 Any conflict between this Agreement and any of the Appendices shall be resolved in favor of this Agreement.

TABLE OF APPENDICES

<u>Appendix</u>	<u>Title</u>
A	Scope of Services
B	Payment Terms
C	Privacy Security and Resilience Agreement

IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day first mentioned above.

CITY OF BERKELEY

By: _____
City Manager

Pre-approved as to form:
CITY ATTORNEY
10/2019

Registered on behalf
of the City Auditor by: _____
Finance Department

Attest by: _____
City Clerk

By: _____
NAME OF PROVIDER

Printed name and title of signatory, if different from Provider name

Taxpayer Identification No. _____

Berkeley Business License No. _____

Incorporated: Yes ___ No ___

Certified Woman Business Enterprise: Yes ___ No ___

Certified Minority Business Enterprise: Yes ___ No ___

If yes, state ethnicity: _____

Certified Disadvantaged Business Enterprise: Yes ___ No ___

APPENDIX A
SCOPE OF SERVICES

APPENDIX B

PAYMENT

APPENDIX C
PRIVACY, SECURITY, AND RESILIENCE

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

1. INFORMATION SECURITY AND PRIVACY

- 1.1. Consultant understands and agrees that, in the performance of the services under this Agreement, Consultant may have access to private or confidential information owned or controlled by City and that such information may contain confidential or proprietary details, the disclosure of which to third parties may be damaging to City.
- 1.2. Consultant’s provision of Hosted Services requires Consultant to collect information that may include confidential and private information from/or about third parties.
 - 1.2.1. Consultant is not authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as privacy data.
 - 1.2.2. Consultant is authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as Health Insurance Portability and Accountability Act (“HIPAA”) regulated data (including records and metadata). City, Consultant, and Consultant’s third-parties (Party) have obligations to protect the privacy and provide for the security of protected health information disclosed to Consultant and their third-parties under this Contract pursuant to HIPAA, the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), and regulations promulgated thereunder including 45 CFR Sections 160 and 164. City and Consultant agree to comply with the Business Associate Addendum (BAA), attached as Exhibit C and made a part of this Contract.
 - 1.2.3. Consultant is authorized by the Agreement to collect, store, disclose or otherwise handle data that is regulated or otherwise recognized by City as privacy data but not Health Insurance Portability and Accountability Act (“HIPAA”) regulated data (including records and metadata). Vendor shall retain data only for deliberate, documented purposes. Vendor shall ensure that the longest retention period any privacy data is subject to dictates the end of that data’s business purpose defined by City and this Agreement
- 1.3. Consultant will store the information on a secure remote server using reasonable safeguards in accordance with the Security Standards of the Agreement codified in DATA SECURITY (Section 2 below) and Consultant’s published on-line privacy policies and in compliance with applicable laws, codes of practice, and other legal obligations associated with the collection, use, and disclosure of personal information. Consultant shall exercise the same standard of care to protect such information as a reasonably prudent Consultant

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

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

2. DATA SECURITY

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

2.1. ADMINISTRATIVE CONTROLS

- 2.1.1. Security Officer: Appoint a head security officer to be responsible for implementing policies, procedures and internal controls to carry out these Security Standards.
- 2.1.2. Cyber-Resilience Program: Document in a Data Security Guide the Consultant's cyber-resilience program. Consultant's cyber-resilience program will include, at a minimum: (i) physical, administrative and technical security controls; (ii) service interruption and data breach notification procedures (such as runbook) and metrics; (iii) release and system upgrade policy and procedures that include and address cybersecurity; (iv) service and disaster availability procedures (such as runbook) and metrics; and (v) Consultant's security, governance, and compliance policy and procedures applicable to its third-parties.

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

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

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

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

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

2.2. TESTING

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

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

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

2.3. RECORD RETENTION.

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

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

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

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

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

2.4. PHYSICAL CONTROLS

2.4.1. PHYSICAL ACCESS MANAGEMENT

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

- 2.4.1.1. Card Access Control: Use card-access controls to partition physical Secure Areas.
- 2.4.1.2. CCTV coverage: Use CCTV monitoring and recording devices, including motion-activated devices, in all physical Secure Areas containing: hard copies of City private and confidential information, including without limitation our proprietary operational information); servers, transfer switches, telecomm link-lines or card-access system links; access areas to and from general work areas; hardware security modules (HSM) and key management equipment, tokens and codes; and all sensitive/restricted areas.
- 2.4.1.3. Physical security presence: Use guards where Card Access Control and CCTV coverage are not possible or are not industry best practice.
- 2.4.1.4. Security management monitoring: Use supervisors, staff monitoring CCTV, and other overseers of physical security to ensure dual-control of physical Secure Areas.
- 2.4.1.5. Segregate all City’s physical and virtual IT environments, servers, switches and operationally sensitive instances and equipment from those for services and functions Consultant performs for Consultant’s clients and consumers other than City.
- 2.4.1.6. Do not allow Consultant’s outside support-services personnel to access physical Secure Areas. All access to these areas by support services personnel must be controlled, documented and physically accompanied by Consultant’s pre-approved staff.

2.5. TECHNICAL CONTROLS

2.5.1. SYSTEMS AND APPLICATIONS RESILIENCE.

- 2.5.1.1. Consistent Emphasis on Security: Throughout the design, development and distribution (in any medium) of IT environments, service, containers, systems, releases, hardware and software applications and APIs, consistently apply information-security and technology-security considerations, and maintain industry-relevant, state-of-the-art security tools, devices, measures, controls, procedures and practices.
- 2.5.1.2. Fully Documented Features: Develop hardware, software and services – including but not limited to releases of Software-as-a-Service (SaaS), other Cloud-based “as-a-Services” (PaaS, IaaS, DRaaS, etc.), containers and APIs – by using only fully documented features that do not disregard or circumvent these Security Standards, including without limitation, bypassing or blocking security controls. Promptly report to City (during the design phase) any deviations from the foregoing requirement and cooperate with and support City to remove those deviations. If Consultant or City discovers any inadequate or inappropriate security, promptly take corrective action. Cooperate with City if

same decides to block or remove/de-install Consultant's product from City IT until the undocumented features and/or security-threatening deviations are corrected. Ensure that hardware and software developed by agents and third-party contractors also meet these requirements.

- 2.5.1.3. Change and Version Management: Maintain configurations and versions of products or services (including without limitation releases, software, containers, and APIs) through change management and version control. Maintain hard-copy and electronic documents showing the configuration and version control of products and services that Consultant delivers to City under the Agreement. Normally, a Change Control Request (CCR) shall be submitted by Consultant as a notification to the City Change Advisory Board (CAB) – no approval is required. When City testing of the CCR is anticipated or required, Consultant shall submit CCR at least two (2) weeks advanced and CCR must be approved by CAB. CCRs disapproved by CAB cannot be implemented by Consultant.
- 2.5.1.4. Data Back-up: Protect and back-up releases, software containers and APIs, program files and data, and all City's data, including without limitation City's private and confidential information needed for the operation of Agreement-required functions to a secure off-site location (sufficiently distant so as to avoid the effects of an interruption that affects your processing center).
- 2.5.1.5. Continuity: In the event the hosted service or any component thereof is rendered inoperative as a result of a natural or other disaster, continue to meet the terms and requirements of the Agreement through alternative means until your Agreement-required functions are recovered.
- 2.5.1.6. Restoration: In the event the hosted service or any component thereof is rendered inoperative as a result of a natural or other disaster, complete the recovery, resumption, and/or restoration activities as described in Consultant's DR Plan to achieve the Recovery Time Objective (RTO) of each affected function.
- 2.5.1.7. Unrecoverable Disaster: In the event the hosted service or any component thereof is rendered permanently inoperative as a result of a natural or other disaster, Consultant will make all commercially reasonable efforts to facilitate the expeditious restoration of the services. Where Consultant is unable to restore Services in a reasonable timeframe as specified by service-level agreement (SLA), City may exercise its right to terminate the agreement.

2.5.2. LOGICAL ACCESS MANAGEMENT.

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

- 2.5.2.1. Least Privilege: Limits systems access to Workers and resources that are needed to perform specific responsibilities or functions.
- 2.5.2.2. Access Accounts: Assigns an individual account to each Worker who is given systems access. The access account must be authorized through NEXGEN' documented IAM system and registered to the individual Worker.
- 2.5.2.3. Authentication and Authorization Credentials: Requires each access-authorized Worker to use an authentication mechanism and unique credentials (e.g., ID and passcode/password) for that Worker's access account. Prohibits Workers from writing down, from sharing such credentials with anyone, from storing such credential in login scripts or other human-readable forms, from hard-coding such credentials in computers, from placing such credentials in any other locations, or from programming such credentials into function keys without appropriate login controls and encryption protection. Powerful accounts must be afforded strong protection, such as multifactor authentication (MFA/2FA) for administrators.
- 2.5.2.4. Process and Service Accounts: Assigns process and service accounts. Define and classify process and service accounts. Proactively manage, monitor, and control process and service account access by automatically discovering and storing accounts; scheduling credential rotation; audit, analyze, and manage activity; and monitor credentials to quickly detect and respond to suspicious and malicious activity.
- 2.5.2.5. Worker Access Review and Termination: Periodic access reviews that audit and monitor all users, especially those with elevated rights, on the Consultant's systems, and enable the immediate termination of access and privileges as warranted by change of job duties or termination in accordance with the principle of least privilege. The access of City Workers for whom we have given written notice to Consultant must be blocked or the authentication mechanism must otherwise invalidate access attempts within one (1) day of notice. Documentation of access reviews and termination actions must facilitate reporting to and examination by the City.
- 2.5.2.6. Cloud Access Provisioning: Cloud Service Consultants (CSP) support City's use of a Cloud Access Security Broker (CASB), including but not limited to managing an Internet Protocol (IP) whitelist and IPSEC/GRE tunneling, as appropriate, to explicitly restrict and permit traffic into and out of City's instance.

2.5.3. UNAUTHORIZED TRAFFIC

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

- 2.5.3.1. Storage, Handling and Disposal of City Data: Separate and segregate all City private and confidential information received (whether received from the City or from another source), developed or processed under the Agreement from all information other than City data. At a minimum, encrypt all such data in storage and transit following industry standards and as technology permits. Where specified by the City, provide the City the capability to encrypt private and confidential information using City owned and managed key management technologies. Unless The City directs otherwise, properly destroy City private and confidential information when no longer required by the business processes of the Agreement, in accordance with industry best practices, provided that such destruction meets any requirements that the City reasonably specifies.
- 2.5.3.2. Security Vulnerability Notification and Resolution: Subscribe to third-party, industry-recognized security-vulnerability and security-notification services applicable to Consultant's IT used to store, handle or dispose of City private and confidential data. In a timely manner, review associated notifications and patches, test patches, schedule and apply patches, validate patch implementation, and record the findings, results and action taken (scheduled and ad hoc) as a result of these reviews. Include, at a minimum, security vulnerability resolution measures within Consultant's release cycle cadence.
- 2.5.3.3. Security Health Check and Certification: Make viewable to the City any applicable third-party security health/hygiene services and vulnerability/security scoring services to which the Consultant subscribes. At a minimum, make viewable to the City (electronically or as a report) all third-party certifications / attestations.
- 2.5.3.4. Security-Event Monitoring and Management: Continually monitor environments, systems, applications, processes and accounts for actual or potential security intrusions or violations. Promptly notify City according to BREACH NOTIFICATION / INCIDENT REPORTING (Section 2) below if suspicious conditions or activities are detected indicating an actual or potential security intrusion or violation. At City's option, cease, suspend, alter, modify or replace, as reasonably necessary, the products or services to be delivered or performed under the Agreement.

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

3. BREACH NOTIFICATION / INCIDENT REPORTING

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

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

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

- Within 24 hours: Using the suspicious@cityofberkeley.info email address, notify City of Berkeley's Department of Information Technology of the alert and incident. In your notification, report to the City: (i) on the nature of the incident, (ii) estimated impact on us, and (iii) investigative action taken or planned.
- Within 3 business days after the initial incident report: Provide City with a written updated report that summarizes the results of the investigative action and corrective/remedial action taken.
- Upon completion of the investigation: Provide City with a final written report that gives a full accounting of the extent of the security intrusion or security violation; a description of any private and confidential information disclosed,

destroyed, compromised or altered; specific corrective/remedial action taken; all supporting technical documentation that may include without limitation application and system network logs, and the cybersecurity impact on us and our systems.

- 3.3. Suspected Privacy Incident. If you discover or are notified of a Privacy or Information Security Incident relating to Customer Data, Consultant shall, to the extent not prohibited by applicable law and at Consultant's cost and expense: (i) notify City of Berkeley of such Information Security Incident as set forth in section 3.2 (above), (ii) investigate such breach, (iii) inform City of Berkeley of the results of such investigation, and (iv) assist the City of Berkeley and State and Federal Agencies impacted by the breach with their reports, including but not limited to cyber suspicious activity reports (Cyber-SAR) and investigations, (v) assist City of Berkeley in maintaining the privacy and confidentiality of such information, (vi) cooperate in, support and assist City of Berkeley in making required breach notifications.
- 3.3.1. Consultant agrees to reasonably cooperate and coordinate with City of Berkeley concerning: (i) City's investigation, enforcement, monitoring, document preparation, notification requirements, efforts to prevent and mitigate, and reporting concerning Privacy and/or Information Security Incidents and Consultant's and City's compliance with Privacy and Information Security Laws; and (ii) any other activities or duties set forth under this Exhibit for which cooperation between Consultant and City of Berkeley may be reasonably necessary.
- 3.3.2. Any determination regarding the applicability of Information Security Laws or Privacy Laws to a Privacy or Information Security Incident and the scope of the obligations pursuant to such laws shall be within the reasonable discretion of City of Berkeley, and Consultant shall comply with any such reasonable determination.
- 3.3.3. When City of Berkeley elects to contact regulators or law enforcement agencies regarding an a Privacy or Information Security Incident, Consultant agrees to cooperate fully with such regulator or law enforcement agencies and any reasonable decision made by City of Berkeley regarding the scope and goals of any investigation undertaken by such regulator or law enforcement agencies.
- 3.3.4. The content of any filings, communications, notices, press releases or reports related to any Privacy Incident referencing City of Berkeley must be approved by City prior to any publication or communication thereof. If requested by City of Berkeley, Consultant shall provide notice to individuals who's Personal Information was affected by the Privacy Incident in a manner and format mutually agreed upon between Consultant and City, as well as any other third parties, such as regulators, law enforcement agencies and consumer reporting agencies.
- 3.3.5. Consultant further authorizes City of Berkeley, in the City's sole discretion and at the Consultant's sole expense, to provide notice of any reasonably required information and documents concerning any Privacy Incident, to individuals or third parties that may have been affected by the Privacy Incident, as well as to law enforcement authorities, regulators, and consumer reporting agency

- 3.4. Assistance in Litigation or Administrative Proceedings. Consultant shall make itself, and any subcontractors, employees, or agents assisting Consultant in the performance of its obligations under the Contract or Addendum, available to City of Berkeley, at no cost to City of Berkeley, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against City of Berkeley, its directors, officers, or employees based upon a claimed violation of applicable privacy and security laws and regulations except where Consultant or its subcontractor, employee or agent is a named adverse party.

4. CONSULTANT'S THIRD PARTIES

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

- 4.1. Consultant must employ a vendor management and security due diligence program, reasonably approved by the City. Consultant must report to the City any proposed Party that cannot materially fulfil confidentiality or security requirements in this Agreement or the security documentation required by this section. City of Berkeley's cyber security and Department of Information Technology (DoIT) vendor management must review, on a case-by-case basis, each Party proposed by Consultant and approve or disapprove of the proposed Party in accordance with the terms of the Agreement.
- 4.2. Consultant must require each Party to comply with the requirements of the City Of Berkeley's Policies, Standards, and Guidelines and must monitor each such Party to determine compliance with same.
- 4.3. Consultant must monitor and provide ongoing oversight of the performance of each Party. Consultant will report to the City whenever there is a reasonably suspected security incident that could affect City Of Berkeley data or the performance of the Services, or that, in Consultant's reasonable judgment, could negatively affect City Of Berkeley's reputation.

5. RETURN OF CITY DATA

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

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

END APPENDIX C
PRIVACY, SECURITY, AND RESILIENCE