City Council Staff Report

Report Type: Consent Calendar  Meeting Date: 12/1/2014

Summary Title: Fiber-to-the-Premise Master Plan and Wireless Network Plan

Title: Approval of and Authorization for the City Manager to Execute Two Professional Services Contracts with Columbia Telecommunications dba CTC Technology & Energy for Consulting Services for (1) a Fiber-to-the-Premise Master Plan in the Amount of $144,944 and (2) a Complementary Wireless Network Plan in the Amount of $131,650; and Adoption of Budget Amendment Ordinance for FY 2015 to Provide Appropriation in the Amount of $276,594 from Fiber Optics Fund

From: City Manager

Lead Department: IT Department

Recommendation
(1) Council approve and authorize the City Manager to execute two Professional Services contracts in amounts not-to-exceed $144,944 and $131,650 to Columbia Telecommunications, dba CTC Technology & Energy, for a Fiber-to-the-Premise Master Plan and a complementary Wireless Network Plan respectively; and (2) adopt a Budget Amendment Ordinance to allocate funding in the amount of $276,594 from the Fiber Optics Fund Rate Stabilization Reserve to fund the development of the plans.

Executive Summary
Under the Council’s “Technology and the Connected City” initiative launched in February 2013, the City seeks the services of Columbia Telecommunications, dba CTC Technology & Energy (CTC) to develop a Fiber-to-the-Premise (FTTP) Master Plan to build out the existing dark fiber optic backbone system, and develop a complementary Wireless Network Plan with a near-term focus on Wi-Fi, and a long-term consideration of other wireless technologies.

Background
On October 28, 2013, the Council voted 7-0 to approve a recommendation by the Technology and Connected City Committee to issue Requests for Proposals (RFPs) to build out the existing dark fiber optic backbone system (fiber system) and develop a Wireless Network Plan with a near-term focus on Wi-Fi, and a long-term consideration of other wireless technologies (Reference: CMR ID # 4203)
As a first step in developing a FTTP Master Plan, staff recommended conducting an RFP to retain a consulting firm with expertise in developing plans and RFPs for government agencies contemplating building broadband networks. Once the findings and recommendations of the Master Plan are developed and submitted to the Council, Council could decide whether to issue an RFP for a private telecommunications service provider to build and operate a FTTP network in Palo Alto, or for the Council to consider the feasibility of the City building and operating a network on its own.

In addition to developing a FTTP Master Plan, staff recommended conducting an RFP to retain professional services from a wireless communications consulting firm with experience working with local governments to develop the options and plans to build a wireless network. Upon completion of the Wireless Network Plan, the findings and recommendations would be submitted to the Council to assist the Council members with formulating a final vision and direction for the deployment of a wireless network.

Staff recommends use of the Fiber Optic Fund Rate Stabilization Reserve (RSR) to fund the FTTP Master Plan and Wireless Network Plan efforts. As part of the Utilities Advisory Commission Meeting on October 1, 2014, it was reported that the Fiber Optics Fund RSR was projected to be $18.4 million as of the end of Fiscal Year 2014. The original cost estimates for these plans were as follows:

<table>
<thead>
<tr>
<th>Plan</th>
<th>Cost Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTTP Master Plan:</td>
<td>$150,000 - $350,000 (depending on required environmental review)</td>
</tr>
<tr>
<td>Wireless Plan:</td>
<td>$100,000 (up to)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$250,000 - $450,000</strong></td>
</tr>
</tbody>
</table>

**Discussion**

Under the direction of the Chief Information Officer (CIO), staff developed RFPs to retain consulting services for the FTTP Master Plan and Wireless Network Plan. Development of the RFPs was assisted by the members of the Citizen Advisory Committee (CAC) appointed by the City Manager in February 2014, to support the Council’s Technology and the Connected City initiative. On July 3, 2014, the RFPs were issued. The RFP submittal deadline was July 29, 2014.

During the week of September 8, 2014, four vendor interviews were conducted. Based on the scoring of the consultant proposals and in-person interviews, the interview panel selected CTC to recommend to the Council to provide professional consulting services for the FTTP Master Plan and the Wireless Network Plan. CTC is an independent communications and IT engineering consulting firm with more than twenty five (25) years of experience. CTC’s customer base includes federal, state and local government agencies.

Among the above-noted vendor responses to the RFPs, CTC’s written proposals and interview
responses for the FTTP Master Plan and Wireless Network Plan aligned most closely with the City objectives and the tasks identified in the scope of work in the RFPs. Overall, CTC’s written proposals for the FTTP Master Plan and the Wireless Network Plan, and the presentation provided before the interview panel, compared most favorably and added more value than the proposals submitted by the other respondents. These factors were reflected in the scoring by the interview panel participants. CTC will provide two project managers for the FTTP and Wireless Plans and the work will proceed in parallel. The rating criteria developed for the written proposals and interviews included:

1. Quality and completeness of proposal and match with scope of work;
2. Quality, performance, and effectiveness of the services to be provided;
3. Proposed cost to the City and ability to meet a specific timeline;
4. Proposer’s experience, including the experience of staff performing work of a similar nature, including fiber and wireless network design and engineering;
5. Proposer’s ability to develop a Request for Proposal and present findings and recommendations to the Council;
6. Proposer’s compliance with applicable requirements.

Since 2000, CTC has provided the City with professional telecommunication consulting services. These services included: (1) working with the City on cable TV franchise issues; (2) planning for the Institutional Network (I-Net) required under the cable TV franchise; (3) identifying fiber system expansion opportunities with a private fiber-optic company seeking to build in Palo Alto (RCN Telecom), and (4) advising the City on preliminary design concepts for the Palo Alto Unified School District fiber project. CTC’s most recent contract with the City was in 2010-2011, which involved the preparation of a “conceptual plan” for phased, low-risk approaches to expanding the existing fiber system for fiber-to-the-premise and wireless deployments. This work was part of the “Citywide Ultra-High Speed Broadband System Project.” The objective for the conceptual plan was to provide strategic guidance on how the City could expand the fiber system for enhanced municipal and commercial services.

On a national level, CTC has been a leader in working with cities and other government agencies on “gigabit-facilitation strategies.” In 2014, CTC authored “Gigabit Communities” a white paper which provides in-depth technical strategies for facilitating public or private broadband construction in communities. Additionally, in the last few years CTC is also working with public power providers in the area of Smart Grid planning.

CTC’s proposal cost for the FTTP Master Plan is a total amount not-to-exceed $144,944. CTC’s proposal cost for the Wireless Network Plan is a total amount not-to-exceed $131,650.

**Summary of City Bid Process (FTTP Master Plan and Wireless Network Plan)**

<p>| Proposed Duration of Projects: | FTTP Master Plan: 120 days. Wireless Network Plan: 120 days. Projects will proceed simultaneously. |</p>
<table>
<thead>
<tr>
<th>Number of Solicitations Emailed:</th>
<th>Twenty (20). RFPs were also posted on the Fiber to the Home Council’s website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Days to respond:</td>
<td>Nineteen (19) Business Days</td>
</tr>
<tr>
<td>Number of Responses Received:</td>
<td>Nine (9)</td>
</tr>
<tr>
<td>Number of Vendors Interviewed:</td>
<td>Four (4)</td>
</tr>
<tr>
<td>Vendor Selected:</td>
<td>CTC Technology &amp; Energy</td>
</tr>
</tbody>
</table>

**Resource Impact**

A Budget Amendment Ordinance in the amount of $276,594 is requested from the Fiber Optic Fund Rate Stabilization Reserve to cover two professional service contracts, which will reduce the Fiber Optic RSR from $18.4 million to $18.2 million. Approximately 1.75 FTEs are assigned from the IT and Utilities Departments to work with the vendor to complete the FTTP Master Plan and Wireless Network Plan. Future fiscal impacts will be addressed with the Council once the findings and recommendations from the FTTP Master Plan and the Wireless Network Plan are evaluated, and the Council provides further direction on the City’s level of involvement in the implementation of the plans.

**Policy Implications**

These recommendations are consistent with the Telecommunications Policy adopted by the Council in 1997, to facilitate advanced telecommunications services in Palo Alto in an environmentally sound manner (Reference CMR: 369:97-Proposed Telecommunications Policy Statements).

**Relationship between the Technology and the Connected City Initiative and Google Fiber**

The development of the FTTP Master Plan and the Wireless Network Plan is not directly related to the City’s response to the Google Fiber City Checklist and the Council’s approval on August 11, 2014 (Reference CMR ID #4726), of a master Network Hut License Agreement with Google Fiber, the latter of which may allow for the placement of one or two Google “Fiber Huts” on individual city-owned sites, subject to the City Council’s approval of such individual sites and applicable site-specific terms. As the FTTP Master Plan and the Wireless Network Plan are developed, staff will continue to work in parallel with Google Fiber to explore their interest in deploying an ultra-high speed fiber optic network in Palo Alto. If Google decides to move forward with a plan to bring FTTP to the City of Palo Alto, staff will consider any implications to the Council-directed Fiber and Wireless work and will bring recommendations to the City Council.

**Environmental Review**

The development of the FTTP Master Plan and a Wireless Network Plan are exempt from the California Environmental Quality Act pursuant to Title 14 of the California Code of Regulations, Section 15262 because they are feasibility and planning studies.

**Attachments:**
- Attachment A: BAO XXXX - Fiber-to-the Premise and Wireless Network Master Plans (DOC)
- Exhibit A-Contract C15152569-FTTP Master Plan (PDF)
- Exhibit B-Contract C15152568-Wireless Master Plan (PDF)
ORDINANCE NO. XXXX

ORDINANCE OF THE COUNCIL OF THE CITY OF PALO ALTO
AMENDING THE BUDGET FOR THE FISCAL YEAR 2015 IN THE
FIBER OPTICS FUND TO PROVIDE APPROPRIATION OF
$276,594 TO AWARD TWO PROFESSIONAL SERVICE
CONTRACTS TO CTC TECHNOLOGY & ENERGY FOR A FIBER-
TO-THE-PREMISE MASTER PLAN ($144,944) AND A
COMPLEMENTARY WIRELESS NETWORK PLAN ($131,650), AND
TO DECREASE THE FIBER OPTIC FUND RATE STABILIZATION
RESERVE BY $276,594 TO FUND THE CONTRACTS.

The Council of the City of Palo Alto does ordain as follows:

SECTION 1. The Council of the City of Palo Alto finds and
determines as follows:

A. Pursuant to the provisions of Section 12 of Article III of
the Charter of the City of Palo Alto, the Council on June 16, 2014
did adopt a budget for fiscal year 2015; and

B. On October 28, 2013, the City Council approved a
recommendation by the Technology and Connected City Committee to
issue Requests for Proposals to build out the existing dark fiber
optic backbone system through a Fiber-to-the-Premise (FTTP) Master
Plan and develop a Wireless Network Plan with a near-term focus on
Wi-Fi, and a long-term consideration of other wireless
technologies; and

C. During the week of September 8, 2014, four vendor
interviews were conducted, and based on the scoring of written
responses and in-person interviews, the panel selected CTC
Technology & Energy to provide consulting services for the FTTP
Master Plan ($144,944) and the Wireless Network Plan ($131,650); and

D. An appropriation of Two-Hundred Seventy-Six Thousand Five-
Hundred Ninety-Four Dollars ($276,594) is needed to fund the
contracts; and

E. City Council authorization is needed to amend the 2015
budget as hereinafter set forth.

SECTION 2. The sum of Two-Hundred Seventy-Six Thousand Five-
Hundred Ninety-Four Dollars ($276,594) is hereby appropriated for
the Fiber-to-the-Premise Master Plan and Wireless Network Plan, and
the Fiber Optic Fund Rate Stabilization Reserve is reduced by $276,594.

SECTION 3. As provided in Section 2.04.330 of the Palo Alto Municipal Code, this ordinance shall become effective upon adoption.

SECTION 4. The actions taken in this ordinance do not constitute a project requiring environmental review under the California Environmental Quality Act (CEQA).

INTRODUCED AND PASSED:
AYES:
NOES:
ABSTENTIONS:
ABSENT:
ATTEST: APPROVED:

__________________________________________
City Clerk Mayor

APPROVED AS TO FORM:

__________________________________________
City Manager

_______________________________
City Attorney Director of Utilities

Director of Information Technology

Director of Administrative Services
CITY OF PALO ALTO CONTRACT NO. C15152569

AGREEMENT BETWEEN THE CITY OF PALO ALTO
AND COLUMBIA TELECOMMUNICATIONS CORPORATION DBA CTC TECHNOLOGY & ENERGY
FOR PROFESSIONAL SERVICES

This Agreement is entered into on this 1st day of December, 2014, (“Agreement”) by and between the CITY OF PALO ALTO, a California chartered municipal corporation (“CITY”), and COLUMBIA TELECOMMUNICATIONS CORPORATION, (dba CTC Technology & Energy), a Maryland corporation, located at 10613 Concord St. Kensington, MD 20885 (“CONSULTANT”).

RECITALS

The following recitals are a substantive portion of this Agreement.

A. CITY intends to develop a Fiber-to-the-Premise Master Plan (“Master Plan”) and write a Request for Proposal (“RFP”) to build a citywide network (“Project”) and desires to engage a consultant to inventory and assess City assets and infrastructure required to support deployment of a fiber network in connection with the Project (“Services”).

B. CONSULTANT has represented that it has the necessary professional expertise, qualifications, and capability, and all required licenses and/or certifications to provide the Services.

C. CITY in reliance on these representations desires to engage CONSULTANT to provide the Services as more fully described in Exhibit “A”, attached to and made a part of this Agreement.

NOW, THEREFORE, in consideration of the recitals, covenants, terms, and conditions, in this Agreement, the parties agree:

AGREEMENT

SECTION 1. SCOPE OF SERVICES. CONSULTANT shall perform the Services described in Exhibit “A” in accordance with the terms and conditions contained in this Agreement. The performance of all Services shall be to the reasonable satisfaction of CITY.

SECTION 2. TERM.
The term of this Agreement shall be from the date of its full execution through May 30, 2015 unless terminated earlier pursuant to Section 19 of this Agreement.

SECTION 3. SCHEDULE OF PERFORMANCE. Time is of the essence in the performance
of Services under this Agreement. CONSULTANT shall complete the Services within the term of this Agreement and in accordance with the schedule set forth in Exhibit “B”, attached to and made a part of this Agreement. Any Services for which times for performance are not specified in this Agreement shall be commenced and completed by CONSULTANT in a reasonably prompt and timely manner based upon the circumstances and direction communicated to the CONSULTANT. CITY’s agreement to extend the term or the schedule for performance shall not preclude recovery of damages for delay if the extension is required due to the fault of CONSULTANT.

SECTION 4. NOT TO EXCEED COMPENSATION. The compensation to be paid to CONSULTANT for performance of the Services described in Exhibit “A”, including both payment for professional services and reimbursable expenses, shall not exceed One Hundred Thirty Six Thousand Five Hundred Forty Four Dollars ($136,544.00). In the event Reimbursable Expenses are authorized, the total compensation for Reimbursable Expenses shall not exceed Eight Thousand Four Hundred Dollars ($8,400.00). The applicable rates and schedule of payment are set out in Exhibit “C-1”, entitled “HOURLY RATE SCHEDULE,” which is attached to and made a part of this Agreement.

Additional Services, if any, shall be authorized in accordance with and subject to the provisions of Exhibit “C”. CONSULTANT shall not receive any compensation for Additional Services performed without the prior written authorization of CITY. Additional Services shall mean any work that is determined by CITY to be necessary for the proper completion of the Project, but which is not included within the Scope of Services described in Exhibit “A”.

SECTION 5. INVOICES. In order to request payment, CONSULTANT shall submit monthly invoices to the CITY describing the services performed and the applicable charges (including an identification of personnel who performed the services, hours worked, hourly rates, and reimbursable expenses), based upon the CONSULTANT’s billing rates (set forth in Exhibit “C-1”). If applicable, the invoice shall also describe the percentage of completion of each task. The information in CONSULTANT’s payment requests shall be subject to verification by CITY. CONSULTANT shall send all invoices to the City’s project manager at the address specified in Section 13 below. The City will generally process and pay invoices within thirty (30) days of receipt.

SECTION 6. QUALIFICATIONS/STANDARD OF CARE. All of the Services shall be performed by CONSULTANT or under CONSULTANT’s supervision. CONSULTANT represents that it possesses the professional and technical personnel necessary to perform the Services required by this Agreement and that the personnel have sufficient skill and experience to perform the Services assigned to them. CONSULTANT represents that it, its employees and subconsultants, if permitted, have and shall maintain during the term of this Agreement all licenses, permits, qualifications, insurance and approvals of whatever nature that are legally required to perform the Services.

All of the services to be furnished by CONSULTANT under this agreement shall meet the professional standard and quality that prevail among professionals in the same discipline and of similar knowledge and skill engaged in related work throughout California under the same or similar circumstances.
SECTION 7. COMPLIANCE WITH LAWS. CONSULTANT shall keep itself informed of and in compliance with all federal, state and local laws, ordinances, regulations, and orders that may affect in any manner the Project or the performance of the Services or those engaged to perform Services under this Agreement. CONSULTANT shall procure all permits and licenses, pay all charges and fees, and give all notices required by law in the performance of the Services.

SECTION 8. ERRORS/OMISSIONS. CONSULTANT shall correct, at no cost to CITY, any and all errors, omissions, or ambiguities in the work product submitted to CITY, provided CITY gives notice to CONSULTANT. If CONSULTANT has prepared plans and specifications or other design documents to construct the Project, CONSULTANT shall be obligated to correct any and all errors, omissions or ambiguities discovered prior to and during the course of construction of the Project. This obligation shall survive termination of the Agreement.

SECTION 9. COST ESTIMATES. If this Agreement pertains to the design of a public works project, CONSULTANT shall submit estimates of probable construction costs at each phase of design submittal. If the total estimated construction cost at any submittal exceeds ten percent (10%) of the CITY’s stated construction budget, CONSULTANT shall make recommendations to the CITY for aligning the PROJECT design with the budget, incorporate CITY approved recommendations, and revise the design to meet the Project budget, at no additional cost to CITY.

SECTION 10. INDEPENDENT CONTRACTOR. It is understood and agreed that in performing the Services under this Agreement CONSULTANT, and any person employed by or contracted with CONSULTANT to furnish labor and/or materials under this Agreement, shall act as and be an independent contractor and not an agent or employee of the CITY.

SECTION 11. ASSIGNMENT. The parties agree that the expertise and experience of CONSULTANT are material considerations for this Agreement. CONSULTANT shall not assign or transfer any interest in this Agreement nor the performance of any of CONSULTANT’s obligations hereunder without the prior written consent of the city manager. Consent to one assignment will not be deemed to be consent to any subsequent assignment. Any assignment made without the approval of the city manager will be void.

SECTION 12. SUBCONTRACTING.

CONSULTANT shall not subcontract any portion of the work to be performed under this Agreement without the prior written authorization of the city manager or designee.

CONSULTANT shall be responsible for directing the work of any subconsultants and for any compensation due to subconsultants. CITY assumes no responsibility whatsoever concerning compensation. CONSULTANT shall be fully responsible to CITY for all acts and omissions of a subconsultant. CONSULTANT shall change or add subconsultants only with the prior approval of the city manager or his designee.

SECTION 13. PROJECT MANAGEMENT. CONSULTANT will assign Joanne Hovis as the Project Manager to have supervisory responsibility for the performance, progress, and execution of the Services and Andrew Afflerbach as the project engineer to represent CONSULTANT during the day-to-day work on the Project. If circumstances cause the
substitution of the project director, project coordinator, or any other key personnel for any reason, the appointment of a substitute project director and the assignment of any key new or replacement personnel will be subject to the prior written approval of the CITY’s project manager. CONSULTANT, at CITY’s request, shall promptly remove personnel who CITY finds do not perform the Services in an acceptable manner, are uncooperative, or present a threat to the adequate or timely completion of the Project or a threat to the safety of persons or property.

The City’s project manager is Todd Henderson, Information Technology Department, Project Services Division, 250 Hamilton Ave. Palo Alto, CA 94303, Telephone: 650-329-2342. The project manager will be CONSULTANT’s point of contact with respect to performance, progress and execution of the Services. The CITY may designate an alternate project manager from time to time.

SECTION 14. OWNERSHIP OF MATERIALS. Upon delivery, all work product, including without limitation, all writings, drawings, plans, reports, specifications, calculations, documents, other materials and copyright interests developed under this Agreement shall be and remain the exclusive property of CITY without restriction or limitation upon their use. CONSULTANT agrees that all copyrights which arise from creation of the work pursuant to this Agreement shall be vested in CITY, and CONSULTANT waives and relinquishes all claims to copyright or other intellectual property rights in favor of the CITY. Neither CONSULTANT nor its contractors, if any, shall make any of such materials available to any individual or organization without the prior written approval of the City Manager or designee. CONSULTANT makes no representation of the suitability of the work product for use in or application to circumstances not contemplated by the scope of work.

SECTION 15. AUDITS. CONSULTANT will permit CITY to audit, at any reasonable time during the term of this Agreement and for three (3) years thereafter, CONSULTANT’s records pertaining to matters covered by this Agreement. CONSULTANT further agrees to maintain and retain such records for at least three (3) years after the expiration or earlier termination of this Agreement.

SECTION 16. INDEMNITY.

16.1. To the fullest extent permitted by law, CONSULTANT shall protect, indemnify, defend and hold harmless CITY, its Council members, officers, employees and agents (each an “Indemnified Party”) from and against any and all demands, claims, or liability of any nature, including death or injury to any person, property damage or any other loss, including all costs and expenses of whatever nature including attorneys fees, experts fees, court costs and disbursements (“Claims”) that arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of the CONSULTANT, its officers, employees, agents or contractors under this Agreement, regardless of whether or not it is caused in part by an Indemnified Party.

16.2. Notwithstanding the above, nothing in this Section 16 shall be construed to require CONSULTANT to indemnify an Indemnified Party from Claims arising from the active negligence, sole negligence or willful misconduct of an Indemnified Party.

Professional Services
Rev. Feb. 2014
16.3. The acceptance of CONSULTANT’s services and duties by CITY shall not operate as a waiver of the right of indemnification. The provisions of this Section 16 shall survive the expiration or early termination of this Agreement.

**SECTION 17. WAIVERS.** The waiver by either party of any breach or violation of any covenant, term, condition or provision of this Agreement, or of the provisions of any ordinance or law, will not be deemed to be a waiver of any other term, covenant, condition, provisions, ordinance or law, or of any subsequent breach or violation of the same or of any other term, covenant, condition, provision, ordinance or law.

**SECTION 18. INSURANCE.**

18.1. CONSULTANT, at its sole cost and expense, shall obtain and maintain, in full force and effect during the term of this Agreement, the insurance coverage described in Exhibit "D". CONSULTANT and its contractors, if any, shall obtain a policy endorsement naming CITY as an additional insured under any general liability or automobile policy or policies.

18.2. All insurance coverage required hereunder shall be provided through carriers with AM Best’s Key Rating Guide ratings of A-:VII or higher which are licensed or authorized to transact insurance business in the State of California. Any and all contractors of CONSULTANT retained to perform Services under this Agreement will obtain and maintain, in full force and effect during the term of this Agreement, identical insurance coverage, naming CITY as an additional insured under such policies as required above.

18.3. Certificates evidencing such insurance shall be filed with CITY concurrently with the execution of this Agreement. The certificates will be subject to the approval of CITY’s Risk Manager and will contain an endorsement stating that the insurance is primary coverage and will not be canceled, or materially reduced in coverage or limits, by the insurer except after filing with the Purchasing Manager thirty (30) days’ prior written notice of the cancellation or modification. If the insurer cancels or modifies the insurance and provides less than thirty (30) days’ notice to CONSULTANT, CONSULTANT shall provide the Purchasing Manager written notice of the cancellation or modification within two (2) business days of the CONSULTANT’s receipt of such notice. CONSULTANT shall be responsible for ensuring that current certificates evidencing the insurance are provided to CITY’s Purchasing Manager during the entire term of this Agreement.

18.4. The procuring of such required policy or policies of insurance will not be construed to limit CONSULTANT's liability hereunder nor to fulfill the indemnification provisions of this Agreement. Notwithstanding the policy or policies of insurance, CONSULTANT will be obligated for the full and total amount of any damage, injury, or loss caused by or directly arising as a result of the Services performed under this Agreement, including such damage, injury, or loss arising after the Agreement is terminated or the term has expired.

**SECTION 19. TERMINATION OR SUSPENSION OF AGREEMENT OR SERVICES.**

19.1. The City Manager may suspend the performance of the Services, in whole or in part, or terminate this Agreement, with or without cause, by giving ten (10) days prior
written notice thereof to CONSULTANT. Upon receipt of such notice, CONSULTANT will immediately discontinue its performance of the Services.

19.2. CONSULTANT may terminate this Agreement or suspend its performance of the Services by giving thirty (30) days prior written notice thereof to CITY, but only in the event of a substantial failure of performance by CITY.

19.3. Upon such suspension or termination, CONSULTANT shall deliver to the City Manager immediately any and all copies of studies, sketches, drawings, computations, and other data, whether or not completed, prepared by CONSULTANT or its contractors, if any, or given to CONSULTANT or its contractors, if any, in connection with this Agreement. Such materials will become the property of CITY.

19.4. Upon such suspension or termination by CITY, CONSULTANT will be paid for the Services rendered or materials delivered to CITY in accordance with the scope of services on or before the effective date (i.e., 10 days after giving notice) of suspension or termination; provided, however, if this Agreement is suspended or terminated on account of a default by CONSULTANT, CITY will be obligated to compensate CONSULTANT only for that portion of CONSULTANT’s services which are of direct and immediate benefit to CITY as such determination may be made by the City Manager acting in the reasonable exercise of his/her discretion. The following Sections will survive any expiration or termination of this Agreement: 14, 15, 16, 19.4, 20, and 25.

19.5. No payment, partial payment, acceptance, or partial acceptance by CITY will operate as a waiver on the part of CITY of any of its rights under this Agreement.

SECTION 20. NOTICES.

All notices hereunder will be given in writing and mailed, postage prepaid, by certified mail, addressed as follows:

To CITY: Office of the City Clerk
City of Palo Alto
Post Office Box 10250
Palo Alto, CA 94303

With a copy to the Purchasing Manager

To CONSULTANT: Attention of the project director
at the address of CONSULTANT recited above

SECTION 21. CONFLICT OF INTEREST.

21.1. In accepting this Agreement, CONSULTANT covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of the Services.
21.2. CONSULTANT further covenants that, in the performance of this Agreement, it will not employ subconsultants, contractors or persons having such an interest. CONSULTANT certifies that no person who has or will have any financial interest under this Agreement is an officer or employee of CITY; this provision will be interpreted in accordance with the applicable provisions of the Palo Alto Municipal Code and the Government Code of the State of California.

21.3. If the Project Manager determines that CONSULTANT is a “Consultant” as that term is defined by the Regulations of the Fair Political Practices Commission, CONSULTANT shall be required and agrees to file the appropriate financial disclosure documents required by the Palo Alto Municipal Code and the Political Reform Act.

SECTION 22. NONDISCRIMINATION. As set forth in Palo Alto Municipal Code section 2.30.510, CONSULTANT certifies that in the performance of this Agreement, it shall not discriminate in the employment of any person because of the race, skin color, gender, age, religion, disability, national origin, ancestry, sexual orientation, housing status, marital status, familial status, weight or height of such person. CONSULTANT acknowledges that it has read and understands the provisions of Section 2.30.510 of the Palo Alto Municipal Code relating to Nondiscrimination Requirements and the penalties for violation thereof, and agrees to meet all requirements of Section 2.30.510 pertaining to nondiscrimination in employment.

SECTION 23. ENVIRONMENTALLY PREFERRED PURCHASING AND ZERO WASTE REQUIREMENTS. CONSULTANT shall comply with the City’s Environmentally Preferred Purchasing policies which are available at the City’s Purchasing Department, incorporated by reference and may be amended from time to time. CONSULTANT shall comply with waste reduction, reuse, recycling and disposal requirements of the City’s Zero Waste Program. Zero Waste best practices include first minimizing and reducing waste; second, reusing waste and third, recycling or composting waste. In particular, Consultant shall comply with the following zero waste requirements:

- All printed materials provided by Consultant to City generated from a personal computer and printer including but not limited to, proposals, quotes, invoices, reports, and public education materials, shall be double-sided and printed on a minimum of 30% or greater post-consumer content paper, unless otherwise approved by the City’s Project Manager. Any submitted materials printed by a professional printing company shall be a minimum of 30% or greater post-consumer material and printed with vegetable based inks.
- Goods purchased by Consultant on behalf of the City shall be purchased in accordance with the City’s Environmental Purchasing Policy including but not limited to Extended Producer Responsibility requirements for products and packaging. A copy of this policy is on file at the Purchasing Office.
- Reusable/returnable pallets shall be taken back by the Consultant, at no additional cost to the City, for reuse or recycling. Consultant shall provide documentation from the facility accepting the pallets to verify that pallets are not being disposed.

SECTION 24. NON-APPROPRIATION

24.1. This Agreement is subject to the fiscal provisions of the Charter of the City of Palo Alto and the Palo Alto Municipal Code. This Agreement will terminate without any
penalty (a) at the end of any fiscal year in the event that funds are not appropriated for the following fiscal year, or (b) at any time within a fiscal year in the event that funds are only appropriated for a portion of the fiscal year and funds for this Agreement are no longer available. This section shall take precedence in the event of a conflict with any other covenant, term, condition, or provision of this Agreement.

SECTION 25. MISCELLANEOUS PROVISIONS.

25.1. This Agreement will be governed by the laws of the State of California.

25.2. In the event that an action is brought, the parties agree that trial of such action will be vested exclusively in the state courts of California in the County of Santa Clara, State of California.

25.3. The prevailing party in any action brought to enforce the provisions of this Agreement may recover its reasonable costs and attorneys' fees expended in connection with that action. The prevailing party shall be entitled to recover an amount equal to the fair market value of legal services provided by attorneys employed by it as well as any attorneys’ fees paid to third parties.

25.4. This document represents the entire and integrated agreement between the parties and supersedes all prior negotiations, representations, and contracts, either written or oral. This document may be amended only by a written instrument, which is signed by the parties.

25.5. The covenants, terms, conditions and provisions of this Agreement will apply to, and will bind, the heirs, successors, executors, administrators, assignees, and consultants of the parties.

25.6. If a court of competent jurisdiction finds or rules that any provision of this Agreement or any amendment thereto is void or unenforceable, the unaffected provisions of this Agreement and any amendments thereto will remain in full force and effect.

25.7. All exhibits referred to in this Agreement and any addenda, appendices, attachments, and schedules to this Agreement which, from time to time, may be referred to in any duly executed amendment hereto are by such reference incorporated in this Agreement and will be deemed to be a part of this Agreement.

25.8 If, pursuant to this contract with CONSULTANT, City shares with CONSULTANT personal information as defined in California Civil Code section 1798.81.5(d) about a California resident (“Personal Information”), CONSULTANT shall maintain reasonable and appropriate security procedures to protect that Personal Information, and shall inform City immediately upon learning that there has been a breach in the security of the system or in the security of the Personal Information. CONSULTANT shall not use Personal Information for direct marketing purposes without City’s express written consent.

25.9 All unchecked boxes do not apply to this agreement.

25.10 The individuals executing this Agreement represent and warrant that they have the legal capacity and authority to do so on behalf of their respective legal entities.
This Agreement may be signed in multiple counterparts, which shall, when executed by all the parties, constitute a single binding agreement.

IN WITNESS WHEREOF, the parties hereto have by their duly authorized representatives executed this Agreement on the date first above written.

CITY OF PALO ALTO

City Manager

APPROVED AS TO FORM:

Senior Deputy, City Attorney

COLUMBIA TELECOMMUNICATIONS CORPORATION dba CTC
TECHNOLOGY AND ENERGY

Attachments:

EXHIBIT “A”: SCOPE OF SERVICES
EXHIBIT “B”: SCHEDULE OF PERFORMANCE
EXHIBIT “C”: COMPENSATION
EXHIBIT “C-1”: SCHEDULE OF RATES
EXHIBIT “D”: INSURANCE REQUIREMENTS
EXHIBIT “E”: SOFTWARE AS A SERVICE
EXHIBIT “F”: VENDOR INFORMATION SECURITY ASSESSMENT
EXHIBIT “G”: INFORMATION PRIVACY POLICY
EXHIBIT “A”
SCOPE OF SERVICES

Background
The City of Palo Alto (“City” or “Palo Alto”) needs assistance from Columbia Communications Corporation dba CTC Technology and Energy (“Consultant”), a Maryland corporation, to develop a Fiber-to-the-Premise Master Plan (“Master Plan”) and assist the City in writing a Request for Proposal (“RFP”) to build a citywide network. Development of this plan is a key part of the City’s “Technology and the Connected City” initiative started by the Mayor and the City Council in March of 2013. The principal objective of the Master Plan is for the City to collect information and data that will guide the evaluation of the best approach for Palo Alto becoming a “Gigabit Community” by building out its 41-mile dark fiber optic backbone system (“fiber system”) to provide citywide access to a Fiber-to-the-Premise Network (“FTTP Network”).

The primary objectives of the Master Plan are to:
1. Provide the City with essential information and data to set its goals and objectives to facilitate the deployment of a FTTP Network in Palo Alto;
2. Develop an inventory and assessment of City assets and infrastructure required to support the deployment of a FTTP Network;
3. Evaluate the impacts a FTTP Network will have on City rights-of-way, City-owned utility poles, conduits, streetlight poles, Fiber System and real property;
4. Define and evaluate FTTP Network requirements;
5. Define services and technologies offered on the FTTP Network;
6. Prepare an engineering study and FTTP Network design, deployment cost model and potential business models to build and operate a citywide network;
7. Provide the City Council with findings and recommendations regarding the feasibility of building a FTTP Network and the best business model to pursue this goal;
8. Assist City staff in writing the RFP based on City Council review and approval of the findings and recommendations in the Master Plan, and further direction from the Council to proceed with issuing an RFP to build a citywide FTTP Network.

Statement of Work
Services from the Consultant include the completion of six (6) tasks, for an amount not to exceed $144,944 ($136,544 not to exceed price amount, plus $8,400 in travel expenses). See Exhibit “C” (Compensation).

The Consultant will complete the following tasks:
1. Inventory and assess City assets and infrastructure required to support deployment of FTTP Network;
2. Evaluate the impacts the construction of a FTTP Network will have on City rights-of-way, utility poles, streetlight poles, conduits, fiber system, real property and other assets and
infrastructure, and the various agreements that govern the use of this infrastructure and real property. Evaluate the various construction methods to build a FTTP Network;

3. Define and evaluate FTTP Network requirements for the RFP;

4. Define and evaluate potential FTTP business models, vendors, services and technologies;

5. Based on completing tasks 1-4, prepare an engineering study and FTTP network design, cost model and evaluate potential business models to implement a citywide FTTP Network in Palo Alto;

6. Present the findings and recommendations for the Master Plan to the City Council, Utilities Advisory Commission, Citizen Advisory Committee and executive City staff. Contingent on City Council direction to proceed, assist City staff with writing an RFP to build a FTTP Network.

Deliverables

Task 1
Inventory and assess City assets and infrastructure required to support deployment of a FTTP Network:
Prepare a written report with an assessment of City assets and infrastructure required to support an FTTP Network. The objective of Task 1 is to review city assets, infrastructure, data and information required to facilitate the preparation of an engineering study, network design, deployment cost model, and potential business models for a FTTP Network. The information and data available from the City to conduct this assessment is defined in the “City Data Required by Consultant to Perform Analysis to Complete Master Plan” section of this Scope of Services on page 16 of this Agreement.

Task 2
Evaluate the impacts the construction of a FTTP Network will have on City rights-of-way, City-owned and controlled utility poles, conduits, streetlight poles, Fiber System, real property and other assets and infrastructure. Evaluate construction methods that support network deployment:
Prepare a written report with an assessment of City assets and infrastructure required to support an FTTP Network deployment, in addition to providing an evaluation of construction methods that support network deployment. The report should evaluate the impacts the construction of a FTTP Network will have on City rights-of-way, City-owned and controlled utility poles, conduits, streetlight poles, fiber system, real property and other assets and infrastructure. The report should address the following issues:

1. Assess the use of City-controlled space on utility poles, streetlight poles, conduit and other City-owned properties to build a FTTP network and/or a Wireless Network and evaluate any impacts on the current agreements that govern the use of these facilities and properties. These agreements include:
   a. The City’s Master License Agreement for City-controlled Space on Utility Poles and Streetlight Poles and in Conduit (“MLA”), various MLA exhibits and associated fees for pole attachments and conduit use. The MLA was developed for the installation of distributed antenna systems (“DAS”) for the purpose of
providing wireless communications facilities in Palo Alto. The MLA also
governs future attachments by third parties on utility poles and streetlight poles
and in conduits controlled by the City;
b. The Joint Pole Agreement between the City of Palo Alto and AT&T and any
potential impacts on that agreement by a new facilities-based “attacher” in Palo
Alto;
c. The Joint Pole Agreement between the City, AT&T and PG&E and any
impacts on that agreement by a new facilities-based “attacher” in Palo Alto;
d. The Conduit License Agreement between the City and Comcast;
e. The Master License Agreement for Installation of Underground Facilities in the
City of Palo Alto by and Among the City of Palo Alto, Pacific Bell Telephone
Company (DBA AT&T California), and Comcast Corporation IX, Inc.

2. Assess the impact on the City’s existing fiber system and the commercial dark fiber
customer base if an FTTP Network builder/operator licenses dark fiber from the City;

3. Assess the number of utility poles requiring make-ready work to accommodate another
facilities-based network attaching fiber and associated electronics and equipment in the
communication space or the unrestricted power space;

4. Identify and evaluate innovative construction methods that could be used to expedite and
possibly lower the cost of FTTP construction.

Task 3
Define and evaluate FTTP Network requirements:
Prepare a written report that will define FTTP Network requirements. The following items
should be evaluated and addressed in the report:
1. A network that uses fiber-to-the-premise architecture: The City considers 1 Gbps
symmetrical service as a baseline for a next-generation FTTP Network; however this
evaluation of FTTP architecture should consider a range of symmetrical and
asymmetrical high data rate transmission speeds in the downstream and upstream
direction. The Master Plan should evaluate the feasibility and cost of offering retail
broadband services with a sustained minimum 1 Gbps dedicated symmetrical
transmission speed over each connection provided to each premise, or a scalable network
that could provide a range of data transmission speeds to each premise.

2. A network able to support high quality voice, data and video services, in addition to other
advanced services and applications delivered over ultra-high speed broadband networks.
Examples of other services and applications include: telemedicine, home security, home
monitoring, cloud services, etc.

3. A network with IPv6 capability, and backward compatibility with IPv4;

4. A network that could be deployed and made operational on a phased, demand driven
basis;

5. A network that promotes the long-term economic and community interests and end user
requirements. End user requirements to evaluate are as follows:
Retail and Local Services
a. Residential and business class Internet access services
b. Telephone and customized Internet service plans for enterprises and institutions
c. Hosted VoIP solutions for small business and residential customers
d. Multi-channel video service
e. On-demand video service
f. Locally-produced content
g. Video conferencing
h. Gateways for access to cloud based community applications and “Over-the-Top” services

Public Safety Services
a. Dedicated and secure public safety network
b. Public infrastructure monitoring (e.g., traffic lights, security cameras and cameras on other public structures)
c. Evaluate network resilience and survivability such as solar power and other emergency back-up power and network architecture to ensure operability for at least seven (7) days with no grid power giving prioritization to public safety, critical infrastructure and lifeline services. This evaluation should include an interview of the Police Department Director of Technical Services and the Director of Emergency Services to develop requirements for network performance (QoS) and compliance with U.S. Department of Justice metrics and other public safety and critical infrastructure metrics.

Community Services
a. Development and implementation of a “Smart Grid” program for stakeholders and customers (e.g. digital technology that allows for two-way communication between the utility and its customers and the sensing along transmission lines)
b. Community-generated public service video channels
c. Community health care services network
d. Health information exchange with secure media access
e. Patient center managed telemedicine services
f. Support for a local application developer community
g. Access to cloud-based development environment
h. Access to content distribution network (CDN) development and distribution channels

Task 4
Define and evaluate potential FTTP business models, vendors, services and technologies:

Prepare a written report to address the following:
1. Evaluate potential business models for building and operating public broadband networks. This evaluation should provide an analysis of the pros and cons of each model and examples of how these networks have been implemented by other local governments. Examples of business models include:
   a. “Retail” - City builds and operates an FTTP Network and directly offers video, broadband, phone and other services to residences and businesses;
   b. “Wholesale” or “open access” - separates the ownership of the infrastructure from the delivery of retail services from several ISPs;
   c. “Infrastructure participation” - City makes available for lease selected assets such
as space on City owned and controlled utility poles and communications conduit, dark fiber and City-owned properties;

d. Evaluate the potential for the City to attract a turnkey vendor to design, build and operate a FTTP Network in Palo Alto.

2. Identify categories of potential vendors to deploy a fully operational high-speed communications network using Internet Protocol ("IP") technology which allows users access to the Internet and access to other services as required;

3. Evaluate the pros and cons of Active Ethernet, PON, GPON or WDM/PON technologies to best provide symmetrical gigabit-speed service to households, businesses and institutions throughout Palo Alto. The evaluation should include an assessment of all active and passive infrastructure, including cabling, active field equipment, uninterruptible power supplies, network cross connections, software, ancillary equipment and ongoing maintenance requirements;

4. Provide a technology assessment with a description of the network technologies underlying proposed network solutions. The description should include the following information:
   a. Technologies proposed and the limitations of each technology. If a variety of technologies are evaluated, a discussion of the issues likely to influence the choice of technologies;
   b. Provide details regarding the proposed network design including, but not limited to: network design criteria, network elements, architecture, protocols, system reliability, availability, operations, security and maintenance requirements;
   c. Provide network performance descriptions, including the range of offerings that could be provisioned over the network, the capacity, and applicable features for each proposed solution;

5. Describe the types of services rendered by potential vendors, including system design, engineering, operation, monitoring, maintenance and enhancement, as well as negotiation and execution of access agreements with retail service providers.

**Task 5**

Based on completing tasks 1-4, and in consultation with the City’s Project Manager and assigned City staff, prepare an engineering study and FTTP network design, cost model and provide an evaluation of potential business models to implement a citywide FTTP Network in Palo Alto.

**Task 6**

Prepare a final comprehensive report for the Master Plan and present the findings and recommendations from the Plan to the City Council, Utilities Advisory Commission, and Citizen Advisory Committee and Executive City staff. Contingent on City Council direction to proceed, assist staff in writing an RFP to build a citywide FTTP network.
City Data Required by Consultant to Perform Analysis to Complete Master Plan

Under the auspices of a Non-disclosure Agreement, the City will provide the Consultant with the following information and data to complete the six tasks:

1. Information System (“GIS”) data sets and mapping information for:
   a. Addresses
   b. Streets
   c. Right of Way and Easements
   d. City Boundaries
   e. Parcels or Lot Lines
   f. Utility Poles
   g. Streetlight Poles
   h. Overhead Strand (Guys and Anchors City-owned, Operated or Controlled)
   i. Existing Underground Utility Routes
   j. Manholes
   k. Pavement Condition Index Score by Street
   l. Zoning
   m. Building Footprint

2. Other available information:
   a. Spare conduit available for lease
   b. Dark fiber available for lease
   c. Infrastructure Maintenance Plans for roads and power
   d. Potential Network Hub Site locations by address
   e. Permitting Processes
   f. City of Palo Alto Utilities Rules and Regulations serve as a general reference to Utilities customers and contractors regarding common Utilities activities, such as access to private property and service contracts:
      http://www.cityofpaloalto.org/gov/depts/utl/about/rules.asp
   g. Previous cost estimates for proposed FTTP projects, including engineering plans and reference architecture for proposed networks, cost and revenue information, and broad historical information from previous FTTP business cases.
   h. Past RFPs developed for the design, construction and operation of a citywide ultra-high speed broadband system.
   i. Previous responses to RFPs.
   j. Previous market research and surveys conducted for FTTP and/or the Citywide Ultra-High Speed Broadband System Project.
   k. Local demographic information.

1 On April 29, 2014, the City of Palo Alto City Council adopted Resolution No. 9408 prohibiting disclosure of confidential and proprietary City and utilities-related infrastructure information; such information will only be available under the auspices of a nondisclosure agreement.
EXHIBIT “B”
SCHEDULE OF PERFORMANCE

CONSULTANT shall perform the Services so as to complete each milestone within the number of days/weeks specified below. The time to complete each milestone may be increased or decreased by mutual written agreement of the project managers for CONSULTANT and CITY so long as all work is completed within the term of the Agreement. CONSULTANT shall provide a detailed schedule of work consistent with the schedule below within 2 weeks of receipt of the notice to proceed.

<table>
<thead>
<tr>
<th>Milestones</th>
<th>Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of Days/Weeks</td>
</tr>
<tr>
<td>1. Task 1</td>
<td>30 days</td>
</tr>
<tr>
<td>2. Task 2</td>
<td>15 days</td>
</tr>
<tr>
<td>3. Task 3</td>
<td>15 days</td>
</tr>
<tr>
<td>4. Task 4</td>
<td>15 days</td>
</tr>
<tr>
<td>5. Task 5</td>
<td>15 days</td>
</tr>
<tr>
<td>6. Task 6</td>
<td>30 days</td>
</tr>
</tbody>
</table>

2 References to tasks correspond to the Tasks set forth in Exhibit “A” attached to this Agreement.
EXHIBIT “C”
COMPENSATION

The CITY agrees to compensate the CONSULTANT for professional services performed in accordance with the terms and conditions of this Agreement, and as set forth in the budget schedule below. Compensation shall be calculated based on the hourly rate schedule attached as Exhibit C-1 up to the not to exceed budget amount for each task set forth below.

The compensation to be paid to CONSULTANT under this Agreement for all services described in Exhibit “A” (“Basic Services”) and reimbursable expenses shall not exceed $144,944, of which Reimbursable Expenses shall not exceed $8,400. CONSULTANT agrees to complete all Basic Services, including reimbursable expenses, within this amount. Additional Services are not authorized under this Agreement. Any work performed or expenses incurred for which payment would result in a total exceeding the maximum amount of compensation set forth herein shall be at no cost to the CITY.

CONSULTANT shall perform the tasks and categories of work as outlined and budgeted below. The CITY’s Project Manager may approve in writing the transfer of budget amounts between any of the tasks or categories listed below provided the total compensation for Basic Services, including reimbursable expenses, does not exceed $144,944, of which Reimbursable Expenses shall not exceed $8,400. Additional Services are not authorized under this Agreement.

<table>
<thead>
<tr>
<th>Task</th>
<th>NOT TO EXCEED AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>$20,000</td>
</tr>
<tr>
<td>(Inventory and assess City assets and infrastructure required to support deployment of FTTP Network)</td>
<td></td>
</tr>
<tr>
<td>Task 2</td>
<td>$20,000</td>
</tr>
<tr>
<td>(Evaluate the impacts the construction of a FTTP Network will have on City rights-of-way, utility poles, streetlight poles, conduits, fiber system, real property and other assets and infrastructure, and the various agreements that govern the use of this infrastructure and real property. Evaluate the various construction methods to build a FTTP Network)</td>
<td></td>
</tr>
<tr>
<td>Task 3</td>
<td>$20,000</td>
</tr>
<tr>
<td>(Define and evaluate FTTP Network requirements for the RFP)</td>
<td></td>
</tr>
<tr>
<td>Task 4</td>
<td>$20,000</td>
</tr>
<tr>
<td>(Define and evaluate potential FTTP business models, vendors, services and technologies)</td>
<td></td>
</tr>
<tr>
<td>Task 5</td>
<td>$20,000</td>
</tr>
<tr>
<td>(Based on completing tasks 1-4, prepare an engineering study and FTTP network)</td>
<td></td>
</tr>
</tbody>
</table>

3 References to tasks correspond to the Tasks set forth in Exhibit “A” attached to this Agreement
design, cost model and evaluate potential business models to implement a citywide FTTP Network in Palo Alto)

Task 6 $36,544
(Present the findings and recommendations for the Master Plan to the City Council, Utilities Advisory Commission, Citizen Advisory Committee and executive City staff. Contingent on City Council direction to proceed, assist City staff with writing an RFP to build a FTTP Network)

Sub-total Basic Services $136,544
Reimbursable Expenses $8,400
Total Basic Services and Reimbursable expenses $144,944
Additional Services (Not to Exceed) $0
Maximum Total Compensation $144,944

REIMBURSABLE EXPENSES

The administrative, overhead, secretarial time or secretarial overtime, word processing, photocopying, in-house printing, insurance and other ordinary business expenses are included within the scope of payment for services and are not reimbursable expenses. CITY shall reimburse CONSULTANT for the following reimbursable expenses at cost. Expenses for which CONSULTANT shall be reimbursed are: Travel expenses in an amount not to exceed $8,400.

A. Travel outside the San Francisco Bay area, including transportation and meals, will be reimbursed at actual cost subject to the City of Palo Alto’s policy for reimbursement of travel and meal expenses for City of Palo Alto employees.

B. Long distance telephone service charges, cellular phone service charges, facsimile transmission and postage charges are reimbursable at actual cost.

All requests for payment of expenses shall be accompanied by appropriate backup information. Any expense anticipated to be more than $0 shall be approved in advance by the CITY’s project manager.

ADDITIONAL SERVICES

The CONSULTANT shall provide additional services only by advanced, written authorization from the CITY. The CONSULTANT, at the CITY’s project manager’s request, shall submit a detailed written proposal including a description of the scope of services, schedule, level of effort, and CONSULTANT’s proposed maximum compensation, including reimbursable expense, for such services based on the rates set forth in Exhibit C-1. The additional services scope, schedule and maximum compensation shall be negotiated and agreed to in writing by the CITY’s Project

Professional Services
Rev. Feb. 2014
Manager and CONSULTANT prior to commencement of the services. Payment for additional services is subject to all requirements and restrictions in this Agreement
EXHIBIT “C-1”
SCHEDULE OF RATES

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Labor Categories</th>
<th>Est. Hours</th>
<th>Hourly Rate</th>
<th>Extended Price</th>
<th>Discount</th>
<th>Extended Discount</th>
<th>Discounted Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1:</td>
<td>Inventory and assess City assets</td>
<td>Director of Business Consulting</td>
<td>28</td>
<td>$170.00</td>
<td>$4,760</td>
<td>15%</td>
<td>$744</td>
<td>$4,046</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>40</td>
<td>$160.00</td>
<td>$6,400</td>
<td>15%</td>
<td>$960</td>
<td>$5,440</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>64</td>
<td>$150.00</td>
<td>$9,600</td>
<td>15%</td>
<td>$1,440</td>
<td>$8,160</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 1 – Not including travel TRAVEL</td>
<td>$21,440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 1 w/ TRAVEL</td>
<td>$21,440</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 2:</td>
<td>Evaluate the impacts of FFTP network deployment</td>
<td>Director of Business Consulting</td>
<td>4</td>
<td>$170.00</td>
<td>$680</td>
<td>15%</td>
<td>$102</td>
<td>$578</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>40</td>
<td>$160.00</td>
<td>$6,400</td>
<td>15%</td>
<td>$960</td>
<td>$5,440</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>40</td>
<td>$150.00</td>
<td>$6,000</td>
<td>15%</td>
<td>$900</td>
<td>$5,100</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 2 – Not including travel TRAVEL</td>
<td>$21,118</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 2 w/ TRAVEL</td>
<td>$21,118</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 3:</td>
<td>Define and evaluate FFTP network requirements</td>
<td>Director of Business Consulting</td>
<td>2</td>
<td>$170.00</td>
<td>$340</td>
<td>15%</td>
<td>$51</td>
<td>$289</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>60</td>
<td>$160.00</td>
<td>$9,600</td>
<td>15%</td>
<td>$1,440</td>
<td>$8,160</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>40</td>
<td>$150.00</td>
<td>$6,000</td>
<td>15%</td>
<td>$900</td>
<td>$5,100</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 3 – Not including travel TRAVEL</td>
<td>$13,549</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 3 w/ TRAVEL</td>
<td>$13,549</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 4:</td>
<td>Define and evaluate potential FFTP business models, vendors, services, and technologies</td>
<td>Director of Business Consulting</td>
<td>22</td>
<td>$170.00</td>
<td>$3,740</td>
<td>15%</td>
<td>$561</td>
<td>$3,179</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>144</td>
<td>$160.00</td>
<td>$23,040</td>
<td>15%</td>
<td>$3,456</td>
<td>$19,584</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>120</td>
<td>$150.00</td>
<td>$18,000</td>
<td>15%</td>
<td>$2,700</td>
<td>$15,300</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 4 – Not including travel TRAVEL</td>
<td>$38,063</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 4 w/ TRAVEL</td>
<td>$39,463</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 5:</td>
<td>Prepare FFTP Master Plan, including findings and recommendations from technical and financial tasks</td>
<td>Director of Business Consulting</td>
<td>16</td>
<td>$170.00</td>
<td>$2,720</td>
<td>15%</td>
<td>$408</td>
<td>$2,312</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>80</td>
<td>$160.00</td>
<td>$12,800</td>
<td>15%</td>
<td>$1,920</td>
<td>$10,880</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>60</td>
<td>$150.00</td>
<td>$9,000</td>
<td>15%</td>
<td>$1,350</td>
<td>$7,650</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 5 – Not including travel TRAVEL</td>
<td>$20,812</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 5 w/ TRAVEL</td>
<td>$22,800</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task 6:</td>
<td>Present recommendations and prepare an RFP for FFTP construction</td>
<td>Director of Business Consulting</td>
<td>40</td>
<td>$170.00</td>
<td>$6,800</td>
<td>15%</td>
<td>$1,020</td>
<td>$5,780</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>116</td>
<td>$160.00</td>
<td>$18,560</td>
<td>15%</td>
<td>$2,790</td>
<td>$15,770</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>108</td>
<td>$150.00</td>
<td>$16,200</td>
<td>15%</td>
<td>$2,430</td>
<td>$13,770</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED</td>
<td>TASK 6 – Not including travel TRAVEL</td>
<td>$35,928</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL TASK 6 w/ TRAVEL</td>
<td>$36,716</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED (TASKS 1 – 6) – Not including travel</td>
<td>$136,544</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED (TASKS 1 – 6) – Travel</td>
<td>$8,400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED (TASKS 1 – 6)</td>
<td>$144,944</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consultant may reallocate funds among task and staff categories with advance notice and approval from City provided the total project cost is not exceeded.
EXHIBIT “D”

INSURANCE REQUIREMENTS

CONTRACTORS TO THE CITY OF PALO ALTO (CITY), AT THEIR SOLE EXPENSE, SHALL FOR THE TERM OF THE CONTRACT OBTAIN AND MAINTAIN INSURANCE IN THE AMOUNTS FOR THE COVERAGE SPECIFIED BELOW, AFFORDED BY COMPANIES WITH AM BEST’S KEY RATING OF A-VII, OR HIGHER, LICENSED OR AUTHORIZED TO TRANSACT INSURANCE BUSINESS IN THE STATE OF CALIFORNIA.

AWARD IS CONTINGENT ON COMPLIANCE WITH CITY’S INSURANCE REQUIREMENTS, AS SPECIFIED, BELOW:

<table>
<thead>
<tr>
<th>REQUIRED</th>
<th>TYPE OF COVERAGE</th>
<th>REQUIREMENT</th>
<th>MINIMUM LIMITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>WORKER’S COMPENSATION</td>
<td>STATUTORY</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>EMPLOYER’S LIABILITY</td>
<td>STATUTORY</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>GENERAL LIABILITY, INCLUDING PERSONAL INJURY, BROAD FORM PROPERTY DAMAGE BLANKET CONTRACTUAL, AND FIRE LEGAL LIABILITY</td>
<td>BODILY INJURY</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROPERTY DAMAGE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BODILY INJURY &amp; PROPERTY DAMAGE COMBINED</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>YES</td>
<td>AUTOMOBILE LIABILITY, INCLUDING ALL OWNED, HIRED, NON-OWNED</td>
<td>BODILY INJURY</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EACH PERSON</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EACH OCCURRENCE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROPERTY DAMAGE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BODILY INJURY AND PROPERTY DAMAGE, COMBINED</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>YES</td>
<td>PROFESSIONAL LIABILITY, INCLUDING, ERRORS AND OMISSIONS, MALPRACTICE (WHEN APPLICABLE), AND NEGLIGENT PERFORMANCE</td>
<td>ALL DAMAGES</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>YES</td>
<td>THE CITY OF PALO ALTO IS TO BE NAMED AS AN ADDITIONAL INSURED: CONTRACTOR, AT ITS SOLE COST AND EXPENSE, SHALL OBTAIN AND MAINTAIN, IN FULL FORCE AND EFFECT THROUGHOUT THE ENTIRE TERM OF ANY RESULTANT AGREEMENT, THE INSURANCE COVERAGE HEREIN DESCRIBED, INSURING NOT ONLY CONTRACTOR AND ITS SUBCONSULTANTS, IF ANY, BUT ALSO, WITH THE EXCEPTION OF WORKERS’ COMPENSATION, EMPLOYER’S LIABILITY AND PROFESSIONAL INSURANCE, NAMING AS ADDITIONAL INSUREDS CITY, ITS COUNCIL MEMBERS, OFFICERS, AGENTS, AND EMPLOYEES.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I. INSURANCE COVERAGE MUST INCLUDE:

A. A PROVISION FOR A WRITTEN THIRTY (30) DAY ADVANCE NOTICE TO CITY OF CHANGE IN COVERAGE OR OF COVERAGE CANCELLATION; AND

B. A CONTRACTUAL LIABILITY ENDORSEMENT PROVIDING INSURANCE COVERAGE FOR CONTRACTOR’S AGREEMENT TO INDEMNIFY CITY.

C. DEDUCTIBLE AMOUNTS IN EXCESS OF $5,000 REQUIRE CITY’S PRIOR APPROVAL.

II. CONTRACTOR MUST SUBMIT CERTIFICATES(S) OF INSURANCE EVIDENCING REQUIRED COVERAGE.

III. ENDORSEMENT PROVISIONS, WITH RESPECT TO THE INSURANCE AFFORDED TO “ADDITIONAL INSUREDS”

A. PRIMARY COVERAGE

WITH RESPECT TO CLAIMS ARISING OUT OF THE OPERATIONS OF THE NAMED INSURED, INSURANCE AS AFFORDED BY THIS POLICY IS PRIMARY AND IS NOT ADDITIONAL TO OR CONTRIBUTING WITH ANY OTHER INSURANCE CARRIED BY OR FOR THE BENEFIT OF THE ADDITIONAL INSUREDS.

B. CROSS LIABILITY
THE NAMING OF MORE THAN ONE PERSON, FIRM, OR CORPORATION AS INSUREDS UNDER THE POLICY SHALL NOT, FOR THAT REASON ALONE, EXTINGUISH ANY RIGHTS OF THE INSURED AGAINST ANOTHER, BUT THIS ENDORSEMENT, AND THE NAMING OF MULTIPLE INSUREDS, SHALL NOT INCREASE THE TOTAL LIABILITY OF THE COMPANY UNDER THIS POLICY.

C. NOTICE OF CANCELLATION

1. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR ANY REASON OTHER THAN THE NON-PAYMENT OF PREMIUM, THE ISSUING COMPANY SHALL PROVIDE CITY AT LEAST A THIRTY (30) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.

2. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR THE NON-PAYMENT OF PREMIUM, THE ISSUING COMPANY SHALL PROVIDE CITY AT LEAST A TEN (10) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.

NOTICES SHALL BE MAILED TO:

PURCHASING AND CONTRACT ADMINISTRATION
CITY OF PALO ALTO
P.O. BOX 10250
PALO ALTO, CA 94303
EXHIBIT “E”

SOFTWARE AS A SERVICE SECURITY AND PRIVACY TERMS AND CONDITIONS

This Exhibit shall be made a part of the City of Palo Alto’s Professional Services Agreement or any other contract entered into by and between the City of Palo Alto (the “City”) and _________________________________ (the “Consultant”) for the provision of Software as a Service to the City (the “Agreement”).

In order to assure the privacy and security of the personal information of the City’s customers and people who do business with the City, including, without limitation, vendors, utility customers, library patrons and other individuals and businesses, who are required to share such information with the City, as a condition of receiving services from the City or selling goods and services to the City, including, without limitation, the Software as a Service services provider (the “Consultant”) and its subcontractors, if any, including, without limitation, any Information Technology (“IT”) infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, described below, while it renders and performs the Services and furnishes goods, if any, described in the Statement of Work, Exhibit B, to the extent any scope of work implicates the confidentiality and privacy of the personal information of the City’s customers. The Consultant shall fulfill the data and information security requirements (the “Requirements”) set forth in Part A below.

A “secure IT environment” includes: (a) the IT infrastructure, by which the Services are provided to the City, including connection to the City’s IT systems; (b) the Consultant’s operations and maintenance processes needed to support the environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. “IT infrastructure” refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

In the event that, after the Effective Date, the Consultant reasonably determines that it cannot fulfill the Requirements, the Consultant shall promptly inform the City of its determination and submit, in writing, one or more alternate countermeasure options to the Requirements (the “Alternate Requirements” as set forth in Part B), which may be accepted or rejected in the reasonable satisfaction of the Information Security Manager (the “ISM”).

Part A. Requirements:

The Consultant shall at all times during the term of any contract between the City and the Consultant:

(a) Appoint or designate an employee, preferably an executive officer, as the security liaison to the City with respect to the Services to be performed under this Agreement.
(b) Provide a full and complete response to the City’s Supplier Security and Privacy Assessment Questionnaire (the “Questionnaire”) to the ISM, and also report any major non-conformance to the Requirements, as and when requested. The response shall include a detailed implementation plan of required countermeasures, which the City requires the Consultant to adopt as countermeasures in the performance of the Services. In addition, as of the annual anniversary date of this Agreement the Consultant shall report to the City, in writing, any major changes to the IT infrastructure.

(c) Have adopted and implemented information security and privacy policies that are documented, are accessible to the City and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards. See the following:

(d) Conduct routine data and information security compliance training of its personnel that is appropriate to their role.

(e) Develop and maintain detailed documentation of the IT infrastructure, including software versions and patch levels.

(f) Develop an independently verifiable process, consistent with industry standards, for performing professional and criminal background checks of its employees that (1) would permit verification of employees’ personal identity and employment status, and (2) would enable the immediate denial of access to the City’s confidential data and information by any of its employees who no longer would require access to that information or who are terminated.

(g) Provide a list of IT infrastructure components in order to verify whether the Consultant has met or has failed to meet any objective terms and conditions.

(h) Implement access accountability (identification and authentication) architecture and support role-base access control (“RBAC”) and segregation of duties (“SoD”) mechanisms for all personnel, systems and software used to provide the Services. “RBAC” refers to a computer systems security approach to restricting access only to authorized users. “SoD” is an approach that would require more than one individual to complete a security task in order to promote the detection and prevention of fraud and errors.

(i) Assist the City in undertaking annually an assessment to assure that: (1) all elements of the Services’ environment design and deployment are known to the City, and (2) it has implemented measures in accordance with industry best practices applicable to secure coding and secure IT architecture.

(j) Provide and maintain secure intersystem communication paths that would ensure the confidentiality, integrity and availability of the City’s information.

(k) Deploy and maintain IT system upgrades, patches and configurations conforming to current patch and/or release levels by not later than one (1) week after its date of release. Emergency security patches must be installed within 24 hours after its date of release.

(l) Provide for the timely detection of, response to, and the reporting of security incidents, including on-going incident monitoring with logging.

(m) Notify the City within one (1) hour of detecting a security incident that results in the unauthorized access to or the misuse of the City’s confidential data and information.

(n) Inform the City that any third party service provider(s) meet(s) all of the Requirements.
(o) Perform security self-audits on a regular basis and not less frequently than on a quarterly basis, and provide the required summary reports of those self-audits to the ISM on the annual anniversary date or any other date agreed to by the Parties.

(p) Accommodate, as practicable, and upon reasonable prior notice by the City, the City’s performance of random site security audits at the Consultant’s site(s), including the site(s) of a third party service provider(s), as applicable. The scope of these audits will extend to the Consultant’s and its third party service provider(s)’ awareness of security policies and practices, systems configurations, access authentication and authorization, and incident detection and response.

(q) Cooperate with the City to ensure that to the extent required by applicable laws, rules and regulations, the Confidential Information will be accessible only by the Consultant and any authorized third party service provider’s personnel.

(r) Perform regular, reliable secured backups of all data needed to maximize availability of the Services.

(s) Maintain records relating to the Services for a period of three (3) years after the expiration or earlier termination of this Agreement and in a mutually agreeable storage medium. Within thirty (30) days after the effective date of expiration or earlier termination of this Agreement, all of those records relating to the performance of the Services shall be provided to the ISM.

(t) Maintain the Confidential Information in accordance with applicable federal, state and local data and information privacy laws, rules and regulations.

(u) Encrypt the Confidential Information before delivering the same by electronic mail to the City and or any authorized recipient.

(v) Unless otherwise addressed in the Agreement, shall not hold the City liable for any direct, indirect or punitive damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the City’s IT environment, including, without limitation, IT infrastructure communications.

Part B. Alternate Requirements:
Vendor Information Security Assessment (VISA) Questionnaire

Purpose: This Vendor Information Security Assessment (VISA) Questionnaire requests information concerning a Cloud Service Provider (the Vendor), which intends to provide to the City of Palo Alto (the City) any or all of the following services: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS).

Note/Instructions:
- SaaS, PaaS and IaaS are each a ‘cloud’ servicing model, in which software and database applications, computer network infrastructure and/or computer hardware/software platforms is/are hosted by the Vendor and made available to customers interconnected in a network, typically the Internet.
- This Questionnaire is for the sole use of the intended Vendor and may contain confidential information of individuals and businesses collected, stored, and used the City. Any unauthorized collection, storage, use, review or distribution may be prohibited by California and/or Federal laws. If you are not the intended recipient of this Questionnaire, please contact the sender by e-mail and destroy all copies of the Questionnaire.
- The Vendor shall provide answers to the questions or information to the requests provided below.
- In the event that the Vendor determines that it cannot meet the City’s security and or privacy requirements, the Vendor may submit a request for an exception to the City’s requirements and propose alternative countermeasures to address the risks addressed in this Questionnaire. The City’s Information Security Manager (ISM) may approve or reject the exception request, depending on the risks associated with the exception request.
- Security Exception Request shall be submitted if you cannot comply with this policy/requirements.
- Upon receipt of the Vendor’s response, the ISM will conduct a security risk assessment, using the following scoring methodology:
  A = Meets completely.
  B = Partially meets. The Vendor may be required to provide additional requested information.
  C = Doesn’t meet. The Vendor may be required to provide missing/additional detail.

Vendor Information:

<table>
<thead>
<tr>
<th>Vendor Organization Name</th>
<th>CTC Inc. Columbia Telecommunications Corporation d/b/a CTC Technology &amp; Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>10613 Concord Street, Kensington, MD 20895</td>
</tr>
<tr>
<td>Information Security Contact Person Name</td>
<td>Matthew DeHaven</td>
</tr>
<tr>
<td>City’s PM</td>
<td>Todd Henderson</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:mdehaven@ctcnet.us">mdehaven@ctcnet.us</a></td>
</tr>
<tr>
<td>Phone</td>
<td>301-933-1488</td>
</tr>
</tbody>
</table>
## 1.0 BUSINESS PROCESS AND DATA EXCHANGE REQUIREMENTS

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Please provide a detailed description of the Vendor’s business process that will be offered to the City, as this relates to the proposed requirements of the City’s RFP or other business requirements</td>
<td>CTC will provide fiber and wireless network design recommendations, strategic planning recommendations, business case analysis, and financial analysis of potential fiber optic and wireless network deployments. The business processes will involve the review and analysis of City infrastructure data, market research, and preparation of network design and business analysis materials.</td>
<td>C</td>
<td>Please provide requested detail</td>
</tr>
<tr>
<td>1.2</td>
<td>Has the Vendor adopted and implemented information security and privacy policies that are documented and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards or NIST 800-53 (National Institute of Standards – NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations)</td>
<td>CTC does not anticipate hosting any applications used by the City or requiring access to City IT resources. Although formal IT security audits are generally not requested by our clients for the type of consulting services we provide, we have in place best-practice security measures consistent with the risk management-based approach to threat mitigation defined by NIST SP 800-53.</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>
| 1.3 | What data exchange will occur between the City and the Vendor? What data will be stored at the Vendor’s or other third party’s data storage location? (Provide data attributes with examples of the data to be stored)

Example: Payment Card Information, Social Security Number, Driving License number, Patrons Name, Address, Telephone etc.), which are examples of personal information, the privacy of which are protected by California constitutional and statutory law. |

We anticipate the data exchange will primarily be through e-mail, and as required due to file attachment size, via commercial “cloud”-based file sharing services (Google Docs, DropBox, etc.). We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materias (e.g. GIS data related to roadway attributes and other City infrastructure). | A |

| 1.4 | In the event that the Vendor is required to store Private Information (PI), Personally Identifiable Information (PII), and Sensitive Information (SI) about individuals/organizations with the service provider’s business systems, how does the Vendor maintain the confidentiality of the information in accordance with applicable federal, state and local data and information privacy laws, rules and regulations? [(The City of Palo Alto (the “City”) strives to promote and sustain a superior quality of life for persons in Palo Alto. In promoting the quality of life of these persons, it is the policy of the City, consistent with the provisions of the California Public Records Act, California Government Code §§ 6250 – 6270, to take]

CTC does not anticipate requiring access to or storing PI, PII, or SI about individuals/organizations. In rare cases when this has been required in the past, CTC has conducted formal IT security audits compliant with client standards, and has successfully implemented risk mitigation plans consistent with these standards. | A |
appropriate measures to safeguard the security and privacy of the personal (including, without limitation, financial) information of persons, collected in the ordinary course and scope of conducting the City’s business as a local government agency. These measures are generally observed by federal, state and local authorities and reflected in federal and California laws, the City’s rules and regulations, and industry best practices, including, without limitation, the provisions of California Civil Code §§ 1798.3(a), 1798.24, 1798.79.8(b), 1798.80(e), 1798.81.5, 1798.82(e), 1798.83(e)(7), and 1798.92(c)].

| 1.5 | What mechanism and/or what types of tool(s) will be used to exchange data between the City and The Vendor? Example: (VPN, Data Link, Frame Relay, HTTP, HTTPS, FTP, FTPS, etc.) | We anticipate primarily transfer of data through email exchange. CTC does not anticipate requiring access to or transmitting PI, PII, or SI about individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materias (e.g. GIS data related to roadway attributes and other City physical infrastructure). Information provided to the City will include conceptual fiber network designs and financial analysis that we expect will be made publically available upon completion. | C | Please advise what data will be processed, provide examples of data to be processed |

<p>| 1.6 | What types of data storage (work in progress storage and backup storage) are present or will be | CTC does not anticipate requiring access to or storing PI, PII, or SI about | A | |</p>
<table>
<thead>
<tr>
<th></th>
<th>required at the Vendor’s site? Example: (PCI Credit Card Info, SSN, DLN, Patrons Name, Address, telephone etc.)</th>
<th>individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materias (e.g. GIS data related to roadway attributes and other City infrastructure).</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7</td>
<td>Is e-mail integration required between the City and the Vendor? Example: The provision of services may require the City to provide the Vendor with an e-mail account on the City’s e-mail server.</td>
<td>CTC does not require integration with the city’s email.</td>
</tr>
<tr>
<td>1.8</td>
<td>Has the Vendor ever been subjected to either an electronic or physical security breach? Please describe the event(s) and the steps taken to mitigate the breach(es). What damages or exposure resulted? Are records of breaches and issues maintained and will these records be available for inspection by the City?</td>
<td>No.</td>
</tr>
<tr>
<td>1.9</td>
<td>Does the Vendor maintain formal security policies and procedures to comply with applicable statutory or industry practice requirements/standards? Are records maintained to demonstrate compliance or certification? Does the Vendor allow client audit of these records? Note: Please submit supporting documentation.</td>
<td>Formal policies are implemented within CTC’s IT infrastructure related to electronic access controls. Statutory and/or industry compliance policies are implemented as-needed on a project basis.</td>
</tr>
<tr>
<td>2.0</td>
<td>What are the internet and the browser security configurations for the cloud application? What security</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### 2.0 APPLICATION/SOLUTION CONFIGURATION

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from The Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from The Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>What is the name of the application(s) that theVendor will be hosting in order to provide services to the City? (List all)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2.2</td>
<td>What functionality will be provided to the City’s employees or the City’s customers or other recipient of City services through the application?</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2.3</td>
<td>Will the Vendor use a subcontractor and/or a third party service provider? (List all). If yes, then what data privacy and information security agreements are in place between the Vendor and any subcontractor/third party to ensure appropriate and accountable treatment of information? Note the City requires that the Vendor and each subcontractor and/or third party formally acknowledge that will</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2.4</td>
<td>What is the Vendor's application(s) hosting hardware and software platform? Provide a detailed description, including security patches or security applications in use. Example: Windows or Unix Operating System (OS) and other detail.</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>How does the Vendor’s application and database architecture to manage or promote segregation of the City's data (related to its function as a local government agency) from the data of individuals providing services to or receiving services from the City?</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>Describe the Vendor’s server and network infrastructure. Please provide server and network infrastructure deployment topology, including data flow architecture, including but not limited to security management applications, firewalls, etc.</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
### 2.7
Please provide a detail proposed solution that will be developed as a part of the Vendor’s implementation to support this project. (For example detailed solution architecture, secured data flow to support business processes, etc.).

<table>
<thead>
<tr>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### 3.0 DATA PROTECTION

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>What will be the medium of data exchange between the City and Vendor?</td>
<td>Primarily email.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>How will the data be kept secure during the data exchange process?</td>
<td>CTC does not anticipate requiring access to or transferring PI, PII, or SI about individuals/organizations. CTC is open to using any preferred transfer solution or technology as deemed appropriate by the City.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>How will the City's data be kept physically and logically secure at the Vendor’s preferred storage location? Example: Locked storage, Digitally, Encrypted etc.</td>
<td>Work materials in progress will be stored on CTC’s internal servers, secured within its headquarters location. The site utilizes electronic keycard access to all doorways, and is protected by an actively monitored electronic security surveillance system. CTC has a formal, documented physical access policy requiring</td>
<td>C</td>
<td>What data transfer is required? Please advise.</td>
</tr>
<tr>
<td>3.4</td>
<td>What application level protections are in place to prevent the Vendor’s or a subcontractor/third party’s staff member from viewing unauthorized confidential information? For example, encryption, masking, etc.</td>
<td>CTC does not anticipate requiring access to or storing PI, PII, or SI about individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materials (e.g. GIS data related to roadway attributes and other City infrastructure). Information provided to the City will include conceptual fiber network designs and financial analysis that we expect will be made publically available upon completion.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>What controls does the Vendor exercise over the qualification and performance of its team? Of their subcontractor/third party’s team(s)? (For example, criminal background)</td>
<td>Our team members undergo a background check and a strict qualification interview that follows closely with the Top Grading interview technique. Qualifications are determined by role/labor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Question</td>
<td>Response</td>
<td>Score</td>
<td>COPA’s Security Assessment</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>4.1</td>
<td>What are the Vendor’s method(s) used to keep data secured during the data backup process?</td>
<td>Offsite data backups are transferred over an AES 256-bit encrypted VPN tunnel.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Is the Vendor’s encryption technology used to encrypt whole or selective data?</td>
<td>All data is encrypted during offsite backup transfer.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>What types of storage media will the Vendor use for data backup purposes? For example, Tape, Hard Disk Drive or any other devices.</td>
<td>Hard Disk Drive.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Are the Vendor’s backup storage devices encrypted? If ‘yes,’ please provide encryption specification, with type of encryption algorithm and detail process of encryption handling. If ‘no,’ provide a detailed description</td>
<td>No, data is not encrypted on storage devices. Offsite data backups are transferred over an AES 256-bit encrypted VPN tunnel. No physical transport of storage media occurs for backups.</td>
<td>B</td>
<td>Depending upon the vendor’s response of the type of data processed we’ll decide the data encryption requirements</td>
</tr>
</tbody>
</table>
(with processes, tools and technology) to keep data secured during the back-up process.

5.0 DATA RETENTION

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>What is the Vendor’s standard data retention period of the backed up data? The data retention process shall comply with the City’s data 7 (seven) years data retention policy. Note: In the event that the Vendor cannot comply with this requirement then the City’s Project Manager shall approval from the City’s data retention schedule/policy owner.</td>
<td>7 years.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>Are the data backup storage media at the Vendor’s location or other third party location?</td>
<td>All backups are stored at a CTC regional location.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>If the Vendor’s backup storage devices are stored with another company, please</td>
<td>N/A</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>What is the media transfer process (i.e. The lock box process used to send tapes off-site)?</td>
<td>Data storage devices are not physically transported. Offsite data backup occurs between CTC locations over AES 256-bit encrypted VPN tunnels.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>Who has access to the data storage media lockbox(es)? (Provide Name and Role)</td>
<td>Only CTC IT Administrators (Matthew DeHaven, CIO/CISO and Eric Wirth, Deputy CIO/CISO)</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>Who on the Vendor’s staff or subcontractor/third party’s staff is/are authorized to access backup data storage media? (Provide Name and Role)</td>
<td>Only CTC IT Administrators (Matthew DeHaven, CIO/CISO and Eric Wirth, Deputy CIO/CISO)</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.8</td>
<td>What is the backup data storage media receipt and release authorization process(es)? (Please submit a soft copy of the process)</td>
<td>N/A</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

6.0 ACCOUNT PROVISIONING AND DE-PROVISIONING (The Vendor must receive formal pre-authorization from the City’s Information Security Manager prior to provisioning and de-provisioning of application access account).
<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>What is the account provisioning/removal process? Example: how are users accounts created and managed?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.2</td>
<td>What is the account deprovisioning/removal process? Example: how are users accounts created and managed?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.3</td>
<td>How will the City’s employees gain access to required application(s)?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.4</td>
<td>Does the application(s) have the capability to restrict access only from the City’s WAN (Wide Area Network)?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

**7.0 PASSWORD MANAGEMENT**

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional</th>
</tr>
</thead>
</table>

VISA Questionnaire
Version 2.0
Page 13 of 16
13 November 2014
<table>
<thead>
<tr>
<th></th>
<th>Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>What will be the policy and/or procedures for the logging, authentication, authorization and password management scheme? (Please provide a soft copy of the process)</td>
</tr>
<tr>
<td>7.2</td>
<td>Where will the login and password credentials be stored?</td>
</tr>
<tr>
<td>7.3</td>
<td>Are the password credentials stored with encryption? If 'yes,' please provide encryption scheme detail.</td>
</tr>
<tr>
<td>7.4</td>
<td>The Vendor’s application must comply with the following password requirements. Does the Vendor’s application meet these requirements?</td>
</tr>
<tr>
<td></td>
<td>1. First time password must be unique to an individual and require the user to change it upon initial login.</td>
</tr>
<tr>
<td></td>
<td>2. If the password is sent via plain text email to the City employee to mitigate security</td>
</tr>
</tbody>
</table>

Please confirm that the City’s employees don’t need to access CTC’s application.
exposure.

3. The City requires first time password to have a time-out capability of no more than 7 days.

4. The e-mail notification must not be copied to anyone except the user.

5. The permanent/long term password must be changed frequently (at least TWICE a year).

6. E-mail notification must be sent to the user whenever the password has been updated.

7. User should not be able to view data or conduct business unless an initial password has been updated with a different password.

8. The Vendor shall inform the City’s users that, when a new password is created, the user shall not use the City’s LDAP (Lightweight Directory Access Control).
9. The password must have 8 or more alphanumeric (/) characters and it must contain at least one character from each of the bullets noted below (i.e. Each line shall contribute at least one character):

- abcdefghijklmnopqrstuvwxyz
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 0123456789
- !@#$%^&*()-+=~>,<\"'?;:{][}
## Information Privacy Policy

<table>
<thead>
<tr>
<th>Release and Version:</th>
<th>1&lt;sup&gt;st&lt;/sup&gt; Release, Version 2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date:</td>
<td>31 January, 2013</td>
</tr>
<tr>
<td>Document Classification:</td>
<td>Need to Know</td>
</tr>
</tbody>
</table>
CONTENTS

DOCUMENT CONTROLS............................................................................................................................................. 2
CHANGE RECORD .......................................................................................................................................................... 2
APPROVAL .................................................................................................................................................................. 2
DISTRIBUTION ............................................................................................................................................................ 2
1. OBJECTIVE ............................................................................................................................................................ 3
   A) INTENT .............................................................................................................................................................. 3
   B) SCOPE ............................................................................................................................................................... 3
   C) CONSEQUENCES............................................................................................................................................... 3
   D) EXCEPTIONS .................................................................................................................................................... 3
   E) MUNICIPAL ORDINANCE ................................................................................................................................... 4

2. RESPONSIBILITIES OF CITY STAFF ..................................................................................................................... 4
   A) RESPONSIBILITY OF CIO AND ISM .................................................................................................................. 4
   B) RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE ......................................................... 4
   C) RESPONSIBILITY OF USERS ............................................................................................................................ 4
   D) RESPONSIBILITY OF INFORMATION TECHNOLOGY (IT) MANAGERS ....................................................... 5
   E) RESPONSIBILITY OF AUTHORIZATION COORDINATION ............................................................................. 5

3. PRIVACY POLICY ..................................................................................................................................................... 5
   A) OVERVIEW ........................................................................................................................................................... 5
   B) PERSONAL INFORMATION AND CHOICE ....................................................................................................... 5
   C) METHODS OF COLLECTION OF PERSONAL INFORMATION ........................................................................ 5
   D) UTILITIES SERVICE .......................................................................................................................................... 6
   E) PUBLIC DISCLOSURE ......................................................................................................................................... 6
   F) ACCESS TO PERSONAL INFORMATION ........................................................................................................ 6
   G) SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE ................................................................................. 6
   H) DATA RETENTION / INFORMATION RETENTION ........................................................................................... 7
   I) SOFTWARE AS A SERVICE (SAAS) OVERSIGHT .......................................................................................... 7
   J) FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003 (FACT) ............................................................. 7

4. CONTACTS ................................................................................................................................................................ 8
DOCUMENT CONTROLS

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Information Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>City of Palo Alto Website and SharePoint</td>
</tr>
<tr>
<td>Document Author</td>
<td>Raj Patel</td>
</tr>
<tr>
<td>Document Manager</td>
<td>Raj Patel</td>
</tr>
<tr>
<td>Contributors</td>
<td>Jonathan Reichental, Shiva Swaminathan, Tom Auzenne, Joe Blackwell, Grant Kolling</td>
</tr>
</tbody>
</table>

CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Jul-12</td>
<td>Raj Patel</td>
<td>0.01</td>
<td>First draft developed</td>
</tr>
<tr>
<td>26-Sep-12</td>
<td>Raj Patel</td>
<td>1.0</td>
<td>First draft released for review</td>
</tr>
<tr>
<td>09-Nov-12</td>
<td>Raj Patel</td>
<td>1.5</td>
<td>Updated first draft for review</td>
</tr>
<tr>
<td>19-Nov-12</td>
<td>Raj Patel</td>
<td>1.6</td>
<td>Additional updates as identified</td>
</tr>
<tr>
<td>22-Nov-12</td>
<td>Raj Patel</td>
<td>1.7</td>
<td>Revised table of content</td>
</tr>
<tr>
<td>26-Nov-12</td>
<td>Raj Patel</td>
<td>1.8</td>
<td>Revised followed by review from Jonathan Reichental and Tom Auzenne</td>
</tr>
<tr>
<td>6-Dec-12</td>
<td>Raj Patel</td>
<td>1.92</td>
<td>Revised according to comments from Jonathan Reichental</td>
</tr>
<tr>
<td>14-Jan-13</td>
<td>Raj Patel</td>
<td>2.0</td>
<td>Revised according to comments from Grant Kolling</td>
</tr>
<tr>
<td>31-Jan-13</td>
<td>Raj Patel</td>
<td>2.2</td>
<td>Revised according to recommendations from Information Security Steering Committee</td>
</tr>
</tbody>
</table>

APPROVAL

| Date       | Name                   | Role                                              | Comments |
|------------|------------------------|                                                  |          |
| 06-Dec-12  | Raj Patel              | Information Security Manager; Information Technology Department | Approved |
| 06-Dec-12  | Jonathan Reichental    | CIO; Information Technology Department           | Approved |
| 06-Dec-12  | Tom Auzenne            | Assistant Director, Utilities Department          | Approved |
| 14-Jan-13  | Grant Kolling          | Senior Assistant City Attorney; City Attorney’s Office | Approved |
| 14-Jan-13  | Information Security Steering Committee | Sponsor | Approved |

DISTRIBUTION

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>City of Palo Alto Employees, Service Providers, Residents and Businesses</td>
<td>City of Palo Alto Website and SharePoint</td>
</tr>
</tbody>
</table>
1. Objective

The City of Palo Alto (the “City”) strives to promote and sustain a superior quality of life for persons in Palo Alto. In promoting the quality of life of these persons, it is the policy of the City, consistent with the provisions of the California Public Records Act, California Government Code §§ 6250 – 6270, to take appropriate measures to safeguard the security and privacy of the personal (including, without limitation, financial) information of persons, collected in the ordinary course and scope of conducting the City’s business as a local government agency. These measures are generally observed by federal, state and local authorities and reflected in federal and California laws, the City’s rules and regulations, and industry best practices, including, without limitation, the provisions of California Civil Code §§ 1798.3(a), 1798.24, 1798.79.8(b), 1798.80(e), 1798.81.5, 1798.82(e), 1798.83(e)(7), and 1798.92(c). Though some of these provisions do not apply to local government agencies like the City, the City will conduct business in a manner which promotes the privacy of personal information, as reflected in federal and California laws. The objective of this Policy is to describe the City’s data security goals and objectives, to ensure the ongoing protection of the Personal Information, Personally Identifiable Information, Protected Critical Infrastructure Information and Personally Identifying Information of persons doing business with the City and receiving services from the City or a third party under contract to the City to provide services. The terms “Personal Information,” “Protected Critical Infrastructure Information”, “Personally Identifiable Information” and “Personally Identifying Information” (collectively, the “Information”) are defined in the California Civil Code sections, referred to above, and are incorporated in this Policy by reference.

A) INTENT

The City, acting in its governmental and proprietary capacities, collects the Information pertaining to persons who do business with or receive services from the City. The Information is collected by a variety of means, including, without limitation, from persons applying to receive services provided by the City, persons accessing the City’s website, and persons who access other information portals maintained by the City’s staff and/or authorized third-party contractors. The City is committed to protecting the privacy and security of the Information collected by the City. The City acknowledges federal and California laws, policies, rules, regulations and procedures, and industry best practices are dedicated to ensuring the Information is collected, stored and utilized in compliance with applicable laws.

The goals and objectives of the Policy are: (a) a safe, productive, and offensive work environment for all users having access to the City’s applications and databases; (b) the appropriate maintenance and security of database information assets owned by, or entrusted to, the City; (c) the controlled access and security of the Information provided to the City’s staff and third party contractors; and (d) faithful compliance with legal and regulatory requirements.

B) SCOPE

The Policy will guide the City’s staff and, indirectly, third party contractors, which are by contract required to protect the confidentiality and privacy of the Information of the persons whose personal information data are intended to be covered by the Policy and which will be advised by City staff to conform their performances to the Policy should they enjoy conditional access to that information.

C) CONSEQUENCES

The City’s employees shall comply with the Policy in the execution of their official duties to the extent their work implicates access to the Information referred to in this Policy. A failure to comply may result in
employment and/or legal consequences.

D) EXCEPTIONS

In the event that a City employee cannot fully comply with one or more element(s) described in this Policy, the employee may request an exception by submitting Security Exception Request. The exception request will be reviewed and administered by the City’s Information Security Manager (the “ISM”). The employee, with the approval of his or her supervisor, will provide any additional information as may be requested by the ISM. The ISM will conduct a risk assessment of the requested exception in accordance with guidelines approved by the City’s Chief Information Officer (“CIO”) and approved as to form by the City Attorney. The Policy’s guidelines will include at a minimum: purpose, source, collection, storage, access, retention, usage, and protection of the Information identified in the request. The ISM will consult with the CIO to approve or deny the exception request. After due consideration is given to the request, the exception request disposition will be communicated, in writing, to the City employee and his or her supervisor. The approval of any request may be subject to countermeasures established by the CIO, acting by the ISM.

E) MUNICIPAL ORDINANCE

This Policy will supersede any City policy, rule, regulation or procedure regarding information privacy.

2. RESPONSIBILITIES OF CITY STAFF

A) RESPONSIBILITY OF CIO AND ISM

The CIO, acting by the ISM, will establish an information security management framework to initiate and coordinate the implementation of information security measures by the City’s government.

The City’s employees, in particular, software application users and database users, and, indirectly, third party contractors under contract to the City to provide services, shall be guided by this Policy in the performance of their job responsibilities.

The ISM will be responsible for: (a) developing and updating the Policy, (b) enforcing compliance with and the effectiveness of the Policy; (c) the development of privacy standards that will manifest the Policy in detailed, auditable technical requirements, which will be designed and maintained by the persons responsible for the City’s IT environments; (d) assisting the City’s staff in evaluating security and privacy incidents that arise in regard to potential violations of the Policy; (e) reviewing and approving department-specific policies and procedures which fall under the purview of this Policy; and (f) reviewing Non-Disclosure Agreements (NDAs) signed by third party contractors, which will provide services, including, without limitation, local or ‘cloud-based’ software services to the City.

B) RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE

The Information Security Steering Committee (the “ISSC”), which is comprised of the City’s employees, drawn from the various City departments, will provide the primary direction, prioritization and approval for all information security efforts, including key information security and privacy risks, programs, initiatives and activities. The ISSC will provide input to the information security and privacy strategic planning processes to ensure that information security risks are adequately considered, assessed and addressed at the appropriate City department level.
C) **Responsibility of Users**

All authorized users of the Information will be responsible for complying with information privacy processes and technologies within the scope of responsibility of each user.

D) **Responsibility of Information Technology (IT) Managers**

The City’s IT Managers, who are responsible for internal, external, direct and indirect connections to the City’s networks, will be responsible for configuring, maintaining and securing the City’s IT networks in compliance with the City’s information security and privacy policies. They are also responsible for timely internal reporting of events that may have compromised network, system or data security.

E) **Responsibility of Authorization Coordination**

The ISM will ensure that the City’s employees secure the execution of Non-Disclosure Agreements (NDA), whenever access to the Information will be granted to third party contractors, in conjunction with the Software as a Service (SaaS) Security and Privacy Terms and Conditions. An NDA must be executed prior to the sharing of the Information of persons covered by this Policy with third party contractors. The City’s approach to managing information security and its implementation (i.e. objectives, policies, processes, and procedures for information security) will be reviewed independently by the ISM at planned intervals, or whenever significant changes to security implementation have occurred.

The CIO, acting by the ISM, will review and recommend changes to the Policy annually, or as appropriate, commencing from the date of its adoption.

3. **Privacy Policy**

A) **Overview**

The Policy applies to activities that involve the use of the City’s information assets, namely, the Information of persons doing business with the City or receiving services from the City, which are owned by, or entrusted to, the City and will be made available to the City’s employees and third party contractors under contract to the City to provide Software as a Service consulting services. These activities include, without limitation, accessing the Internet, using e-mail, accessing the City’s intranet or other networks, systems, or devices.

The term “information assets” also includes the personal information of the City’s employees and any other related organizations while those assets are under the City’s control. Security measures will be designed, implemented, and maintained to ensure that only authorized persons will enjoy access to the information assets. The City’s staff will act to protect its information assets from theft, damage, loss, compromise, and inappropriate disclosure or alteration. The City will plan, design, implement and maintain information management systems, networks and processes in order to assure the appropriate confidentiality, integrity, and availability of its information assets to the City’s employees and authorized third parties.

B) **Personal Information and Choice**

Except as permitted or provided by applicable laws, the City will not share the Information of any person doing business with the City, or receiving services from the City, in violation of this Policy, unless that person has consented to the City’s sharing of such information during the conduct of the City’s business as a local government agency with third parties under contract to the City to provide services.
C) METHODS OF COLLECTION OF PERSONAL INFORMATION

The City may gather the Information from a variety of sources and resources, provided that the collection of such information is both necessary and appropriate in order for the City to conduct business as a local government agency in its governmental and proprietary capacities. That information may be gathered at service windows and contact centers as well as at web sites, by mobile applications, and with other technologies, wherever the City may interact with persons who need to share such formation in order to secure the City’s services.

The City’s staff will inform the persons whose Information are covered by this Policy that the City’s web site may use “cookies” to customize the browsing experience with the City of Palo Alto web site. The City will note that a cookie contains unique information that a web site can use to track, among others, the Internet Protocol address of the computer used to access the City’s web sites, the identification of the browser software and operating systems used, the date and time a user accessed the site, and the Internet address of the website from which the user linked to the City’s web sites. Cookies created on the user’s computer by using the City’s web site do not contain the Information, and thus do not compromise the user’s privacy or security. Users can refuse the cookies or delete the cookie files from their computers by using any of the widely available methods. If the user chooses not to accept a cookie on his or her computer, it will not prevent or prohibit the user from gaining access to or using the City’s sites.

D) UTILITIES SERVICE

In the provision of utility services to persons located within Palo Alto, the City of Palo Alto Utilities Department (“CPAU”) will collect the Information in order to initiate and manage utility services to customers. To the extent the management of that information is not specifically addressed in the Utilities Rules and Regulations or other ordinances, rules, regulations or procedures, this Policy will apply; provided, however, any such Rules and Regulations must conform to this Policy, unless otherwise directed or approved by the Council. This includes the sharing of CPAU-collected Information with other City departments except as may be required by law.

Businesses and residents with standard utility meters and/or having non-metered monthly services will have secure access through a CPAU website to their Information, including, without limitation, their monthly utility usage and billing data. In addition to their regular monthly utilities billing, businesses and residents with non-standard or experimental electric, water or natural gas meters may have their usage and/or billing data provided to them through non-City electronic portals at different intervals than with the standard monthly billing.

Businesses and residents with such non-standard or experimental metering will have their Information covered by the same privacy protections and personal information exchange rules applicable to Information under applicable federal and California laws.

E) PUBLIC DISCLOSURE

The Information that is collected by the City in the ordinary course and scope of conducting its business could be incorporated in a public record that may be subject to inspection and copying by the public, unless such information is exempt from disclosure to the public by California law.

F) ACCESS TO PERSONAL INFORMATION

The City will take reasonable steps to verify a person’s identity before the City will grant anyone online access to that person’s Information. Each City department that collects Information will afford access to affected persons who can review and update that information at reasonable times.
G) SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE

Except as otherwise provided by applicable law or this Policy, the City will treat the Information of persons covered by this Policy as confidential and will not disclose it, or permit it to be disclosed, to third parties without the express written consent of the person affected. The City will develop and maintain reasonable controls that are designed to protect the confidentiality and security of the Information of persons covered by this Policy.

The City may authorize the City’s employee and or third party contractors to access and/or use the Information of persons who do business with the City or receive services from the City. In those instances, the City will require the City’s employee and/or the third party contractors to agree to use such Information only in furtherance of City-related business and in accordance with the Policy.

If the City becomes aware of a breach, or has reasonable grounds to believe that a security breach has occurred, with respect to the Information of a person, the City will notify the affected person of such breach in accordance with applicable laws. The notice of breach will include the date(s) or estimated date(s) of the known or suspected breach, the nature of the Information that is the subject of the breach, and the proposed action to be taken or the responsive action taken by the City.

H) DATA RETENTION / INFORMATION RETENTION

The City will store and secure all Information for a period of time as may be required by law, or if no period is established by law, for seven (7) years, and thereafter such information will be scheduled for destruction.

I) SOFTWARE AS A SERVICE (SaaS) OVERSIGHT

The City may engage third party contractors and vendors to provide software application and database services, commonly known as Software-as-a-Service (SaaS).

In order to assure the privacy and security of the Information of those who do business with the City and those who received services from the City, as a condition of selling goods and/or services to the City, the SaaS services provider and its subcontractors, if any, including any IT infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, while it performs such services and/or furnishes goods to the City, to the extent any scope of work or services implicates the confidentiality and privacy of the Information.

These requirements include information security directives pertaining to: (a) the IT infrastructure, by which the services are provided to the City, including connection to the City's IT systems; (b) the SaaS services provider’s operations and maintenance processes needed to support the IT environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. The term “IT infrastructure” refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

Prior to entering into an agreement to provide services to the City, the City’s staff will require the SaaS services provider to complete and submit an Information Security and Privacy Questionnaire. In the event that the SaaS services provider reasonably determines that it cannot fulfill the information security requirements during the course of providing services, the City will require the SaaS services provider to promptly inform the ISM.

J) FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

CPAU will require utility customers to provide their Information in order for the City to initiate and manage utility services to them.
Federal regulations, implementing the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), including the Red Flag Rules, require that CPAU, as a “covered financial institution or creditor” which provides services in advance of payment and which can affect consumer credit, develop and implement procedures for an identity theft program for new and existing accounts to detect, prevent, respond and mitigate potential identity theft of its customers' Information.

CPAU procedures for potential identity theft will be reviewed independently by the ISM annually or whenever significant changes to security implementation have occurred. The ISM will recommend changes to CPAU identity theft procedures, or as appropriate, so as to conform to this Policy.

There are California laws which are applicable to identity theft; they are set forth in California Civil Code § 1798.92.

4. CONTACTS

Information Security Manager: Patel, Raj <Raj.Patel@CityofPaloAlto.org>
Chief Information Officer: Reichental, Jonathan <Jonathan.Reichental@CityofPaloAlto.org>
Utilities Department: Auzenne, Tom <Tom.Auzenne@CityofPaloAlto.org>
City Attorney’s Office: Kolling, Grant <Grant.Kolling@CityofPaloAlto.org>
CITY OF PALO ALTO CONTRACT NO. C15152568

AGREEMENT BETWEEN THE CITY OF PALO ALTO AND

COLUMBIA TELECOMMUNICATIONS CORPORATION

DBA CTC TECHNOLOGY & ENERGY

FOR PROFESSIONAL SERVICES

This Agreement is entered into on this 1st day of December, 2014, (“Agreement”) by and between the CITY OF PALO ALTO, a California chartered municipal corporation (“CITY”), and COLUMBIA TELECOMMUNICATIONS CORPORATION (dba CTC Technology & Energy), a Maryland corporation, located at 10613 Concord St. Kensington, MD 20885 (“CONSULTANT”).

RECITALS

The following recitals are a substantive portion of this Agreement.

A. CITY intends to develop a Wireless Network Plan with a near-term focus on Wi-Fi deployment and a long-term consideration of other wireless technologies (“Project”) and desires to engage a consultant to inventory and assess City assets and infrastructure required to support deployment of a wireless network in connection with the Project (“Services”).

B. CONSULTANT has represented that it has the necessary professional expertise, qualifications, and capability, and all required licenses and/or certifications to provide the Services.

C. CITY in reliance on these representations desires to engage CONSULTANT to provide the Services as more fully described in Exhibit “A”, attached to and made a part of this Agreement.

NOW, THEREFORE, in consideration of the recitals, covenants, terms, and conditions, in this Agreement, the parties agree:

AGREEMENT

SECTION 1. SCOPE OF SERVICES. CONSULTANT shall perform the Services described in Exhibit “A” in accordance with the terms and conditions contained in this Agreement. The performance of all Services shall be to the reasonable satisfaction of CITY.

SECTION 2. TERM.
The term of this Agreement shall be from the date of its full execution through May 30, 2015 unless terminated earlier pursuant to Section 19 of this Agreement.
**SECTION 3. SCHEDULE OF PERFORMANCE.** Time is of the essence in the performance of Services under this Agreement. CONSULTANT shall complete the Services within the term of this Agreement and in accordance with the schedule set forth in Exhibit “B”, attached to and made a part of this Agreement. Any Services for which times for performance are not specified in this Agreement shall be commenced and completed by CONSULTANT in a reasonably prompt and timely manner based upon the circumstances and direction communicated to the CONSULTANT. CITY’s agreement to extend the term or the schedule for performance shall not preclude recovery of damages for delay if the extension is required due to the fault of CONSULTANT.

**SECTION 4. NOT TO EXCEED COMPENSATION.** The compensation to be paid to CONSULTANT for performance of the Services described in Exhibit “A”, including both payment for professional services and reimbursable expenses, shall not exceed One Hundred Twenty Three Thousand Two Hundred Fifty Dollars ($123,250.00). In the event Reimbursable Expenses are authorized, the total compensation for Reimbursable Expenses shall not exceed Eight Thousand Four Hundred Dollars ($8,400.00). The applicable rates and schedule of payment are set out in Exhibit “C-1”, entitled “HOURLY RATE SCHEDULE,” which is attached to and made a part of this Agreement.

Additional Services, if any, shall be authorized in accordance with and subject to the provisions of Exhibit “C”. CONSULTANT shall not receive any compensation for Additional Services performed without the prior written authorization of CITY. Additional Services shall mean any work that is determined by CITY to be necessary for the proper completion of the Project, but which is not included within the Scope of Services described in Exhibit “A”.

**SECTION 5. INVOICES.** In order to request payment, CONSULTANT shall submit monthly invoices to the CITY describing the services performed and the applicable charges (including an identification of personnel who performed the services, hours worked, hourly rates, and reimbursable expenses), based upon the CONSULTANT’s billing rates (set forth in Exhibit “C-1”). If applicable, the invoice shall also describe the percentage of completion of each task. The information in CONSULTANT’s payment requests shall be subject to verification by CITY. CONSULTANT shall send all invoices to the City’s project manager at the address specified in Section 13 below. The City will generally process and pay invoices within thirty (30) days of receipt.

**SECTION 6. QUALIFICATIONS/STANDARD OF CARE.** All of the Services shall be performed by CONSULTANT or under CONSULTANT’s supervision. CONSULTANT represents that it possesses the professional and technical personnel necessary to perform the Services required by this Agreement and that the personnel have sufficient skill and experience to perform the Services assigned to them. CONSULTANT represents that it, its employees and subconsultants, if permitted, have and shall maintain during the term of this Agreement all licenses, permits, qualifications, insurance and approvals of whatever nature that are legally required to perform the Services.

All of the services to be furnished by CONSULTANT under this agreement shall meet the professional standard and quality that prevail among professionals in the same discipline and of similar knowledge and skill engaged in related work throughout California under the same or similar circumstances.
SECTION 7. COMPLIANCE WITH LAWS. CONSULTANT shall keep itself informed of and in compliance with all federal, state and local laws, ordinances, regulations, and orders that may affect in any manner the Project or the performance of the Services or those engaged to perform Services under this Agreement. CONSULTANT shall procure all permits and licenses, pay all charges and fees, and give all notices required by law in the performance of the Services.

SECTION 8. ERRORS/OMISSIONS. CONSULTANT shall correct, at no cost to CITY, any and all errors, omissions, or ambiguities in the work product submitted to CITY, provided CITY gives notice to CONSULTANT. If CONSULTANT has prepared plans and specifications or other design documents to construct the Project, CONSULTANT shall be obligated to correct any and all errors, omissions or ambiguities discovered prior to and during the course of construction of the Project. This obligation shall survive termination of the Agreement.

SECTION 9. COST ESTIMATES. If this Agreement pertains to the design of a public works project, CONSULTANT shall submit estimates of probable construction costs at each phase of design submittal. If the total estimated construction cost at any submittal exceeds ten percent (10%) of the CITY’s stated construction budget, CONSULTANT shall make recommendations to the CITY for aligning the PROJECT design with the budget, incorporate CITY approved recommendations, and revise the design to meet the Project budget, at no additional cost to CITY.

SECTION 10. INDEPENDENT CONTRACTOR. It is understood and agreed that in performing the Services under this Agreement CONSULTANT, and any person employed by or contracted with CONSULTANT to furnish labor and/or materials under this Agreement, shall act as and be an independent contractor and not an agent or employee of the CITY.

SECTION 11. ASSIGNMENT. The parties agree that the expertise and experience of CONSULTANT are material considerations for this Agreement. CONSULTANT shall not assign or transfer any interest in this Agreement nor the performance of any of CONSULTANT’s obligations hereunder without the prior written consent of the city manager. Consent to one assignment will not be deemed to be consent to any subsequent assignment. Any assignment made without the approval of the city manager will be void.

SECTION 12. SUBCONTRACTING. CONSULTANT shall not subcontract any portion of the work to be performed under this Agreement without the prior written authorization of the city manager or designee.

CONSULTANT shall be responsible for directing the work of any subconsultants and for any compensation due to subconsultants. CITY assumes no responsibility whatsoever concerning compensation. CONSULTANT shall be fully responsible to CITY for all acts and omissions of a subconsultant. CONSULTANT shall change or add subconsultants only with the prior approval of the city manager or his designee.

SECTION 13. PROJECT MANAGEMENT. CONSULTANT will assign Andrew Afflerbach as the Project Manager to have supervisory responsibility for the performance, progress, and execution of the Services to represent CONSULTANT during the day-to-day work.
on the Project. If circumstances cause the substitution of the project director, project coordinator, or any other key personnel for any reason, the appointment of a substitute project director and the assignment of any key new or replacement personnel will be subject to the prior written approval of the CITY’s project manager. CONSULTANT, at CITY’s request, shall promptly remove personnel who CITY finds do not perform the Services in an acceptable manner, are uncooperative, or present a threat to the adequate or timely completion of the Project or a threat to the safety of persons or property.

The City’s project manager is Todd Henderson, Information Technology Department, Project Services Division, 250 Hamilton Ave. Palo Alto, CA 94303, Telephone: 650-329-2342. The project manager will be CONSULTANT’s point of contact with respect to performance, progress and execution of the Services. The CITY may designate an alternate project manager from time to time.

SECTION 14. OWNERSHIP OF MATERIALS. Upon delivery, all work product, including without limitation, all writings, drawings, plans, reports, specifications, calculations, documents, other materials and copyright interests developed under this Agreement shall be and remain the exclusive property of CITY without restriction or limitation upon their use. CONSULTANT agrees that all copyrights which arise from creation of the work pursuant to this Agreement shall be vested in CITY, and CONSULTANT waives and relinquishes all claims to copyright or other intellectual property rights in favor of the CITY. Neither CONSULTANT nor its contractors, if any, shall make any of such materials available to any individual or organization without the prior written approval of the City Manager or designee. CONSULTANT makes no representation of the suitability of the work product for use in or application to circumstances not contemplated by the scope of work.

SECTION 15. AUDITS. CONSULTANT will permit CITY to audit, at any reasonable time during the term of this Agreement and for three (3) years thereafter, CONSULTANT’s records pertaining to matters covered by this Agreement. CONSULTANT further agrees to maintain and retain such records for at least three (3) years after the expiration or earlier termination of this Agreement.

SECTION 16. INDEMNITY.

16.1. To the fullest extent permitted by law, CONSULTANT shall protect, indemnify, defend and hold harmless CITY, its Council members, officers, employees and agents (each an “Indemnified Party”) from and against any and all demands, claims, or liability of any nature, including death or injury to any person, property damage or any other loss, including all costs and expenses of whatever nature including attorneys fees, experts fees, court costs and disbursements (“Claims”) that arise out of, pertain to, or relate to the negligence, recklessness, or willful misconduct of the CONSULTANT, its officers, employees, agents or contractors under this Agreement, regardless of whether or not it is caused in part by an Indemnified Party.

16.2. Notwithstanding the above, nothing in this Section 16 shall be construed to require CONSULTANT to indemnify an Indemnified Party from Claims arising from the active negligence, sole negligence or willful misconduct of an Indemnified Party.
16.3. The acceptance of CONSULTANT’s services and duties by CITY shall not operate as a waiver of the right of indemnification. The provisions of this Section 16 shall survive the expiration or early termination of this Agreement.

SECTION 17. WAIVERS. The waiver by either party of any breach or violation of any covenant, term, condition or provision of this Agreement, or of the provisions of any ordinance or law, will not be deemed to be a waiver of any other term, covenant, condition, provisions, ordinance or law, or of any subsequent breach or violation of the same or of any other term, covenant, condition, provision, ordinance or law.

SECTION 18. INSURANCE.

18.1. CONSULTANT, at its sole cost and expense, shall obtain and maintain, in full force and effect during the term of this Agreement, the insurance coverage described in Exhibit "D". CONSULTANT and its contractors, if any, shall obtain a policy endorsement naming CITY as an additional insured under any general liability or automobile policy or policies.

18.2. All insurance coverage required hereunder shall be provided through carriers with AM Best’s Key Rating Guide ratings of A-:VII or higher which are licensed or authorized to transact insurance business in the State of California. Any and all contractors of CONSULTANT retained to perform Services under this Agreement will obtain and maintain, in full force and effect during the term of this Agreement, identical insurance coverage, naming CITY as an additional insured under such policies as required above.

18.3. Certificates evidencing such insurance shall be filed with CITY concurrently with the execution of this Agreement. The certificates will be subject to the approval of CITY’s Risk Manager and will contain an endorsement stating that the insurance is primary coverage and will not be canceled, or materially reduced in coverage or limits, by the insurer except after filing with the Purchasing Manager thirty (30) days’ prior written notice of the cancellation or modification. If the insurer cancels or modifies the insurance and provides less than thirty (30) days’ notice to CONSULTANT, CONSULTANT shall provide the Purchasing Manager written notice of the cancellation or modification within two (2) business days of the CONSULTANT’s receipt of such notice. CONSULTANT shall be responsible for ensuring that current certificates evidencing the insurance are provided to CITY’s Purchasing Manager during the entire term of this Agreement.

18.4. The procuring of such required policy or policies of insurance will not be construed to limit CONSULTANT's liability hereunder nor to fulfill the indemnification provisions of this Agreement. Notwithstanding the policy or policies of insurance, CONSULTANT will be obligated for the full and total amount of any damage, injury, or loss caused by or directly arising as a result of the Services performed under this Agreement, including such damage, injury, or loss arising after the Agreement is terminated or the term has expired.

SECTION 19. TERMINATION OR SUSPENSION OF AGREEMENT OR SERVICES.

19.1. The City Manager may suspend the performance of the Services, in whole or in part, or terminate this Agreement, with or without cause, by giving ten (10) days prior
written notice thereof to CONSULTANT. Upon receipt of such notice, CONSULTANT will immediately discontinue its performance of the Services.

19.2. CONSULTANT may terminate this Agreement or suspend its performance of the Services by giving thirty (30) days prior written notice thereof to CITY, but only in the event of a substantial failure of performance by CITY.

19.3. Upon such suspension or termination, CONSULTANT shall deliver to the City Manager immediately any and all copies of studies, sketches, drawings, computations, and other data, whether or not completed, prepared by CONSULTANT or its contractors, if any, or given to CONSULTANT or its contractors, if any, in connection with this Agreement. Such materials will become the property of CITY.

19.4. Upon such suspension or termination by CITY, CONSULTANT will be paid for the Services rendered or materials delivered to CITY in accordance with the scope of services on or before the effective date (i.e., 10 days after giving notice) of suspension or termination; provided, however, if this Agreement is suspended or terminated on account of a default by CONSULTANT, CITY will be obligated to compensate CONSULTANT only for that portion of CONSULTANT’s services which are of direct and immediate benefit to CITY as such determination may be made by the City Manager acting in the reasonable exercise of his/her discretion. The following Sections will survive any expiration or termination of this Agreement: 14, 15, 16, 19.4, 20, and 25.

19.5. No payment, partial payment, acceptance, or partial acceptance by CITY will operate as a waiver on the part of CITY of any of its rights under this Agreement.

SECTION 20. NOTICES.

All notices hereunder will be given in writing and mailed, postage prepaid, by certified mail, addressed as follows:

To CITY: Office of the City Clerk
          City of Palo Alto
          Post Office Box 10250
          Palo Alto, CA 94303

          With a copy to the Purchasing Manager

To CONSULTANT: Attention of the project director
                      at the address of CONSULTANT recited above

SECTION 21. CONFLICT OF INTEREST.

21.1. In accepting this Agreement, CONSULTANT covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of the Services.
21.2. CONSULTANT further covenants that, in the performance of this Agreement, it will not employ subconsultants, contractors or persons having such an interest. CONSULTANT certifies that no person who has or will have any financial interest under this Agreement is an officer or employee of CITY; this provision will be interpreted in accordance with the applicable provisions of the Palo Alto Municipal Code and the Government Code of the State of California.

21.3. If the Project Manager determines that CONSULTANT is a “Consultant” as that term is defined by the Regulations of the Fair Political Practices Commission, CONSULTANT shall be required and agrees to file the appropriate financial disclosure documents required by the Palo Alto Municipal Code and the Political Reform Act.

SECTION 22. NONDISCRIMINATION. As set forth in Palo Alto Municipal Code section 2.30.510, CONSULTANT certifies that in the performance of this Agreement, it shall not discriminate in the employment of any person because of the race, skin color, gender, age, religion, disability, national origin, ancestry, sexual orientation, housing status, marital status, familial status, weight or height of such person. CONSULTANT acknowledges that it has read and understands the provisions of Section 2.30.510 of the Palo Alto Municipal Code relating to Nondiscrimination Requirements and the penalties for violation thereof, and agrees to meet all requirements of Section 2.30.510 pertaining to nondiscrimination in employment.

SECTION 23. ENVIRONMENTALLY PREFERRED PURCHASING AND ZERO WASTE REQUIREMENTS. CONSULTANT shall comply with the City’s Environmentally Preferred Purchasing policies which are available at the City’s Purchasing Department, incorporated by reference and may be amended from time to time. CONSULTANT shall comply with waste reduction, reuse, recycling and disposal requirements of the City’s Zero Waste Program. Zero Waste best practices include first minimizing and reducing waste; second, reusing waste and third, recycling or composting waste. In particular, Consultant shall comply with the following zero waste requirements:

- All printed materials provided by Consultant to City generated from a personal computer and printer including but not limited to, proposals, quotes, invoices, reports, and public education materials, shall be double-sided and printed on a minimum of 30% or greater post-consumer content paper, unless otherwise approved by the City’s Project Manager. Any submitted materials printed by a professional printing company shall be a minimum of 30% or greater post-consumer material and printed with vegetable based inks.

- Goods purchased by Consultant on behalf of the City shall be purchased in accordance with the City’s Environmental Purchasing Policy including but not limited to Extended Producer Responsibility requirements for products and packaging. A copy of this policy is on file at the Purchasing Office.

- Reusable/returnable pallets shall be taken back by the Consultant, at no additional cost to the City, for reuse or recycling. Consultant shall provide documentation from the facility accepting the pallets to verify that pallets are not being disposed.

SECTION 24. NON-APPROPRIATION

24.1. This Agreement is subject to the fiscal provisions of the Charter of the
City of Palo Alto and the Palo Alto Municipal Code. This Agreement will terminate without any penalty (a) at the end of any fiscal year in the event that funds are not appropriated for the following fiscal year, or (b) at any time within a fiscal year in the event that funds are only appropriated for a portion of the fiscal year and funds for this Agreement are no longer available. This section shall take precedence in the event of a conflict with any other covenant, term, condition, or provision of this Agreement.

SECTION 25. MISCELLANEOUS PROVISIONS.

25.1. This Agreement will be governed by the laws of the State of California.

25.2. In the event that an action is brought, the parties agree that trial of such action will be vested exclusively in the state courts of California in the County of Santa Clara, State of California.

25.3. The prevailing party in any action brought to enforce the provisions of this Agreement may recover its reasonable costs and attorneys' fees expended in connection with that action. The prevailing party shall be entitled to recover an amount equal to the fair market value of legal services provided by attorneys employed by it as well as any attorneys’ fees paid to third parties.

25.4. This document represents the entire and integrated agreement between the parties and supersedes all prior negotiations, representations, and contracts, either written or oral. This document may be amended only by a written instrument, which is signed by the parties.

25.5. The covenants, terms, conditions and provisions of this Agreement will apply to, and will bind, the heirs, successors, executors, administrators, assignees, and consultants of the parties.

25.6. If a court of competent jurisdiction finds or rules that any provision of this Agreement or any amendment thereto is void or unenforceable, the unaffected provisions of this Agreement and any amendments thereto will remain in full force and effect.

25.7. All exhibits referred to in this Agreement and any addenda, appendices, attachments, and schedules to this Agreement which, from time to time, may be referred to in any duly executed amendment hereto are by such reference incorporated in this Agreement and will be deemed to be a part of this Agreement.

25.8 If, pursuant to this contract with CONSULTANT, City shares with CONSULTANT personal information as defined in California Civil Code section 1798.81.5(d) about a California resident (“Personal Information”), CONSULTANT shall maintain reasonable and appropriate security procedures to protect that Personal Information, and shall inform City immediately upon learning that there has been a breach in the security of the system or in the security of the Personal Information. CONSULTANT shall not use Personal Information for direct marketing purposes without City’s express written consent.

25.9 All unchecked boxes do not apply to this agreement.
25.10 The individuals executing this Agreement represent and warrant that they have the legal capacity and authority to do so on behalf of their respective legal entities.

25.11 This Agreement may be signed in multiple counterparts, which shall, when executed by all the parties, constitute a single binding agreement.

IN WITNESS WHEREOF, the parties hereto have by their duly authorized representatives executed this Agreement on the date first above written.

CITY OF PALO ALTO

____________________________
City Manager

COLUMBIA TELECOMMUNICATIONS
CORPORATION dba CTC
TECHNOLOGY AND ENERGY

____________________________
Joanne Haris

APPROVED AS TO FORM:

____________________________
Senior Deputy City Attorney

Attachments:

EXHIBIT “A”: SCOPE OF SERVICES
EXHIBIT “B”: SCHEDULE OF PERFORMANCE
EXHIBIT “C”: COMPENSATION
EXHIBIT “C-1”: SCHEDULE OF RATES
EXHIBIT “D”: INSURANCE REQUIREMENTS
EXHIBIT “E”: SOFTWARE AS A SERVICE
EXHIBIT “F”: VENDOR INFORMATION SECURITY ASSESSMENT
EXHIBIT “G”: INFORMATION PRIVACY POLICY
EXHIBIT “A”
SCOPE OF SERVICES

Background
The City of Palo Alto (“City” or “Palo Alto”) needs assistance from Columbia Communications Corporation dba CTC Technology and Energy (“Consultant”) to develop a Wireless Network Plan (“Plan”) and assist the City in writing a Request for Proposal (“RFP”) to build a citywide network. The City wants to develop a Plan with a near-term focus on Wi-Fi deployment and a long-term consideration of other wireless technologies.

The primary objectives of the Plan are to evaluate the following:
1. Wi-Fi broadband connectivity for the general public and businesses to ensure economic development, increased access to broadband and digital inclusion for all members of the community;
2. Improved wireless broadband connectivity to support public safety and the delivery of municipal services by field-based staff using a wide variety of mobile government applications over tablets, laptops and smartphones;
3. Wireless government to improve efficiency and reduce the cost of public administration.

Statement of Work
Services from the Consultant include five (5) tasks, for an amount not to exceed $131,650 ($123,250 not to exceed price amount, plus $8,400 in travel expenses). See Exhibit “C” (Compensation).

Deliverables
The following tasks describe the City’s expectations regarding the areas that should be addressed to assist the City in developing a Wireless Network Plan:

Task 1
Prepare a written report defining the fundamental action steps required to develop a wireless broadband initiative for the City, including an assessment of how the existing Fiber System and other supporting municipal infrastructure can be leveraged and maximized to deploy Wi-Fi and/or a citywide wireless network. This task should provide examples of communities that have developed effective municipal wireless networks and how these networks are used to enhance the delivery of municipal services, in addition to providing the general public and businesses with some level of wireless broadband connectivity, either as an “amenity grade” Wi-Fi service in certain areas of the community or as a citywide service that may be subscription-based.

Task 2
Conduct a user group “needs assessment” for a wireless network among all City departments and also assess the need for an amenity-grade or subscription-based Wi-Fi service for the general public and businesses. The primary purpose of the needs assessment is to define the City’s strategic priorities and operational needs driving the overall design standards for either a multi-use network for public safety, municipal service delivery and public access, or a network with a more limited scope. Examples of City departments with field-based staff who may benefit from access to a multi-use municipal wireless network include:
• Planning and Building (Building Inspectors and Code Enforcement Officers)
• Community Services (Open Spaces and Recreation Staff)
• Public Works (Engineers, Inspectors and construction crews)
• Utilities (Engineers, Estimators, Inspectors and construction crews)
• Public Safety departments (Police, Office of Emergency Services and Fire) to support connectivity of field staff as well as the 911 Center and Emergency Operation Center, located in the Police Department.1

The user group needs assessment should also take into account an evaluation of the communication approaches to implement Smart Grid applications such as Advanced Metering Infrastructure (AMI) and Smart Meters. This assessment should include a review of the findings and recommendations described in the “Assessment of Smart Grid Applications for the City of Palo Alto” Final Report prepared by EnerNex Corporation (February 2011) (the”Final EnerNex Report”) (See, specifically, Section 4.2.3 “Proposed Smart Grid Communications Architecture” and Sec. 6.0 “Evaluation of Communication Systems Approaches” of the Final EnerNex Report. City provided the Final EnerNex Report to Consultant as Attachment J to the Wireless Network Plan Request for Proposal - No. 152568, and additional electronic copies of the report can be made available by City upon request from Consultant.

CPAU is currently conducting a Customer Connect Smart Grid Pilot Project. CPAU has deployed a 900 MHz mesh network which covers approximately 75 percent of the geographic area of Palo Alto to serve the 300 residential customers participating in the pilot dispersed throughout Palo Alto. The cost of setting up this network was under $20,000. This network is capable of remotely reading and monitoring customer electric, natural gas and water meters. Monitoring devices are set up along the distribution network in a non-SCADA configuration. It is presently estimated that with equipment it is worth an additional $30,000-$50,000. The network could be expanded to cover 100 percent of the city to read all 29,000 customer accounts and 72,000 customer meters. If the pilot project proves to be successful by the end of 2015, this radio-based mesh network, along with cellular phone based backhaul, will be a strong candidate for a communication network for Smart Grid applications. Task 2 should also include an assessment of alternatives to the commercial cellular networks currently used by the City for mobile broadband access. The objective is to meet the City’s long term needs for public safety first responders and other field-based staff dependent on reliable, high data rate mobile broadband connectivity to effectively deliver municipal services. This assessment should compare and contrast the current commercial cellular network’s strengths and weaknesses against those of a citywide multi-use Wi-Fi WAN.

Prepare a written report based on the findings of the user-group needs assessment.

Task 3

1 Police vehicles and fire apparatus, and other field-based City staff, currently use commercial cellular networks for mobile broadband access. Public safety vehicles are equipped with Mobile Data Computers (MDCs) that provide Internet access and run a variety of specialized public safety applications, including Computer Aided Dispatch (CAD), GIS-based mapping application, and CALPHOTO, which provides officers with a photo to identify individuals. To switch from one network to another, police and fire vehicles are equipped with NetMotion software which allows the MDCs to roam between cellular and Wi-Fi networks seamlessly depending on signal strength.
Based on the user group needs assessment, recommend wireless technology options and design considerations for either a multi-use network (municipal, public safety and public access), or a network with a more limited scope. Design considerations should include an assessment and recommendations of the following:

1. Review available City-owned assets and infrastructure to support the mounting of antennas and equipment for a Wi-Fi and/or wireless network. Assets and infrastructure include the potential use of City-controlled public rights-of-way, availability of spare dark fiber for wireless access points to support network backhaul, space on utility poles and streetlight poles, and available space in conduit. The City also has approximately 90 fiber-connected traffic signals, in addition to communication towers and multiple City-owned properties and buildings;

2. Evaluate and recommend network architecture and technology choices (e.g., Wi-Fi, 2.4/5.8 GHz Wi-Fi system, WiMAX, 4.9 GHz public safety band and 4G cellular) based on the City’s overall wireless goals and the findings identified in the user group needs assessment;

3. Evaluate and recommend wireless technology and network architecture that is flexible and scalable to meet the City’s short term objectives and also able to adapt to emerging services and applications over time;

4. Evaluate network topology based on the scope of the network and integration with the fiber system, internal data networks, and the various applications used by field-based staff;

5. Evaluate and recommend network hardware and software components required to support end users;

6. Identify potential project vendors based on network technology choices and design priorities. Examples of these vendors include: network designers, field installation contractors, application developers, systems integrators and Internet Service Providers (ISPs);

7. Define network security criteria and features and make a recommendation;

8. Develop network cost estimates based on the results of the user needs assessment, technology choices and the scope of the project;

9. Evaluate the integration of a wireless network with existing City computer systems, databases and various enterprise applications;

10. Define operational Information Technology items such as the need for a Subscriber Management System and ongoing support structures, including customer Service Level Agreements;

11. Identify the skill sets required by the City’s Information Technology and Utilities Departments to implement and operate a wireless network;

12. Define and evaluate network resilience and survivability design goals, including solar power and other emergency back-up power and network architecture operability for at least seven (7) days with no grid power, with prioritization to public safety, critical infrastructure and lifeline services. To complete the evaluation, interview the Police Department Director of Technical Services, the Director of Emergency Services and the
Utilities Department Director of Engineering to develop requirements for network performance (QoS) and compliance with United States Department of Justice metrics and other public safety and critical infrastructure metrics.

**Task 4**
Prepare a written report analyzing the advantages and disadvantages of the various business models used to deploy municipal wireless networks and make a recommendation based on the needs of the City and various potential users of the network. This analysis should include a municipal wireless program review of networks deployed in other cities. Potential business models would include, but would not be limited to the following:

1. City-owned wholesale model: the wireless network is owned and operated by the City.
2. Privately-owned managed services model: the wireless network is owned and operated by a service provider, but the City is an “anchor tenant” for the network.
3. Hybrid model (public-private partnership): the City owns the network, but outsources operation and maintenance to a service provider.

Task 4 should also include an assessment of the legal responsibilities under the various business models and general policy development such as VLAN strategies or QoS restrictions and opportunities.

**Task 5**
Upon completion of the Wireless Network Plan, in consultation with City staff, prepare a written report presenting the findings and recommendations to the City Council, Utilities Advisory Commission, Citizen Advisory Committee and executive City staff. Based on the findings and recommendations established in the final Wireless Network Plan, and contingent upon City Council direction to proceed, develop a RFP for a vendor to build a Wi-Fi system and/or a citywide wireless network. The Consultant must consider previous, current, and future planned wireless-related evaluation efforts by the City in order to avoid repeating or duplicating efforts. The City’s Project Manager will assist in identifying and understanding these efforts at the outset of this consulting engagement.

**City Data Required by Consultant to Perform Analysis to Complete Wireless Network Plan**
Under the auspices of a Non-disclosure Agreement, the City will provide the Consultant with the following information and data to complete the six tasks:

1. Information System (“GIS”) data sets and mapping information for:
   a. Addresses
   b. Streets
   c. Right of Way and Easements
   d. City Boundaries
   e. Parcels or Lot Lines
   f. Utility Poles
   g. Streetlight Poles

---

2 On April 29, 2014, the City of Palo Alto City Council adopted Resolution No. 9408 prohibiting disclosure of confidential and proprietary City and utilities-related infrastructure information; such information will only be available under the auspices of a nondisclosure agreement.
h. Overhead Strand (Guys and Anchors City-owned, Operated or Controlled)
i. Existing Underground Utility Routes
j. Manholes
k. Pavement Condition Index Score by Street
l. Zoning
m. Building Footprint

2. Other available information:
a. Spare conduit available for lease
b. Dark fiber available for lease
c. Infrastructure Maintenance Plans for roads and power
d. Potential Network Hub Site locations by address
e. Permitting Processes
f. City of Palo Alto Utilities Rules and Regulations serve as a general reference to Utilities customers and contractors regarding common Utilities activities, such as access to private property and service contracts:
   http://www.cityofpaloalto.org/gov/depts/utl/about/rules.asp
g. Previous cost estimates for proposed wireless projects, including engineering plans and reference architecture for proposed networks, cost and revenue information, and broad historical information from previous wireless business cases and pilot programs.
h. Past RFPs developed for the design, construction and operation of a citywide ultra-high speed broadband network
i. Previous responses to RFPs related to fiber system expansion Wi-Fi and wireless deployment
j. Previous market research and surveys conducted for a wireless network
k. Local demographic information
EXHIBIT “B”
SCHEDULE OF PERFORMANCE

CONSULTANT shall perform the Services so as to complete each milestone within the number of days/weeks specified below. The time to complete each milestone may be increased or decreased by mutual written agreement of the project managers for CONSULTANT and CITY so long as all work is completed within the term of the Agreement. CONSULTANT shall provide a detailed schedule of work consistent with the schedule below within 2 weeks of receipt of the notice to proceed.

<table>
<thead>
<tr>
<th>Milestones</th>
<th>Completion No. of Days/Weeks From NTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Task 1</td>
<td>30 days</td>
</tr>
<tr>
<td>2. Task 2</td>
<td>30 days</td>
</tr>
<tr>
<td>3. Task 3</td>
<td>15 days</td>
</tr>
<tr>
<td>4. Task 4</td>
<td>15 days</td>
</tr>
<tr>
<td>5. Task 5</td>
<td>30 days</td>
</tr>
</tbody>
</table>

3 References to tasks correspond to the Tasks set forth in Exhibit “A” attached to this Agreement.
EXHIBIT “C”
COMPENSATION

The CITY agrees to compensate the CONSULTANT for professional services performed in accordance with the terms and conditions of this Agreement, and as set forth in the budget schedule below. Compensation shall be calculated based on the hourly rate schedule attached as Exhibit C-1 up to the not to exceed budget amount for each task set forth below.

The compensation to be paid to CONSULTANT under this Agreement for all services described in Exhibit “A” (“Basic Services”) and reimbursable expenses shall not exceed $131,650, of which Reimbursable Expenses shall not exceed $8,400. CONSULTANT agrees to complete all Basic Services, including reimbursable expenses, within this amount. Additional Services are not authorized under this Agreement. Any work performed or expenses incurred for which payment would result in a total exceeding the maximum amount of compensation set forth herein shall be at no cost to the CITY.

CONSULTANT shall perform the tasks and categories of work as outlined and budgeted below. The CITY’s Project Manager may approve in writing the transfer of budget amounts between any of the tasks or categories listed below provided the total compensation for Basic Services, including reimbursable expenses, does not exceed $131,650 of which Reimbursable Expenses shall not exceed $8,400. Additional Services are not authorized under this Agreement.

<table>
<thead>
<tr>
<th>BUDGET SCHEDULE</th>
<th>NOT TO EXCEED AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>$20,000</td>
</tr>
<tr>
<td>Task 2</td>
<td>$20,000</td>
</tr>
<tr>
<td>Task 3</td>
<td>$20,000</td>
</tr>
<tr>
<td>Task 4</td>
<td>$20,000</td>
</tr>
<tr>
<td>Task 5</td>
<td>$43,250</td>
</tr>
<tr>
<td>Sub-total Basic Services</td>
<td><strong>$123,250</strong></td>
</tr>
<tr>
<td>Reimbursable Expenses</td>
<td><strong>$8,400</strong></td>
</tr>
<tr>
<td>Total Basic Services and Reimbursable expenses</td>
<td><strong>$131,650</strong></td>
</tr>
<tr>
<td>Additional Services (Not to Exceed)</td>
<td><strong>$0</strong></td>
</tr>
</tbody>
</table>

4 References to tasks correspond to the Tasks set forth in Exhibit “A” attached to this Agreement.
Maximum Total Compensation $131,650

REIMBURSABLE EXPENSES

The administrative, overhead, secretarial time or secretarial overtime, word processing, photocopying, in-house printing, insurance and other ordinary business expenses are included within the scope of payment for services and are not reimbursable expenses. CITY shall reimburse CONSULTANT for the following reimbursable expenses at cost. Expenses for which CONSULTANT shall be reimbursed are: Travel expenses in an amount not to exceed $8,400.

A. Travel outside the San Francisco Bay area, including transportation and meals, will be reimbursed at actual cost subject to the City of Palo Alto’s policy for reimbursement of travel and meal expenses for City of Palo Alto employees.

B. Long distance telephone service charges, cellular phone service charges, facsimile transmission and postage charges are reimbursable at actual cost.

All requests for payment of expenses shall be accompanied by appropriate backup information. Any expense anticipated to be more than $0 shall be approved in advance by the CITY’s project manager.

ADDITIONAL SERVICES

The CONSULTANT shall provide additional services only by advanced, written authorization from the CITY. The CONSULTANT, at the CITY’s project manager’s request, shall submit a detailed written proposal including a description of the scope of services, schedule, level of effort, and CONSULTANT’s proposed maximum compensation, including reimbursable expense, for such services based on the rates set forth in Exhibit C-1. The additional services scope, schedule and maximum compensation shall be negotiated and agreed to in writing by the CITY’s Project Manager and CONSULTANT prior to commencement of the services. Payment for additional services is subject to all requirements and restrictions in this Agreement.
EXHIBIT “C-1”
SCHEDULE OF RATES

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Labor Categories</th>
<th>Est. Hours</th>
<th>Hourly Rate</th>
<th>Extended Rate</th>
<th>Discount</th>
<th>Extended Discount</th>
<th>Discounted Price</th>
<th>Discounted Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1: Conduct system-level requirements analysis</td>
<td>Director of Engineering</td>
<td>0</td>
<td>$170.00</td>
<td>$0</td>
<td>n/a</td>
<td>n/a</td>
<td>$0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>59.3</td>
<td>$160.00</td>
<td>$6,500</td>
<td>15%</td>
<td>$945</td>
<td>$5,555</td>
<td>$118.82</td>
</tr>
<tr>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>39.3</td>
<td>$140.00</td>
<td>$2,700</td>
<td>15%</td>
<td>$405</td>
<td>$2,295</td>
<td>$118.91</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED, TASK 1 - Not including travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$7,650</td>
<td>$118.91</td>
</tr>
<tr>
<td>TRAVEL</td>
<td>Total Task 1 - Including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$9,330</td>
<td>$118.91</td>
</tr>
<tr>
<td></td>
<td>Task 2: Conduct a wireless network needs assessment</td>
<td>20.6</td>
<td>$170.00</td>
<td>$3,500</td>
<td>15%</td>
<td>$525</td>
<td>$3,975</td>
<td>$144.42</td>
</tr>
<tr>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>37.5</td>
<td>$160.00</td>
<td>$4,000</td>
<td>15%</td>
<td>$600</td>
<td>$3,400</td>
<td>$136.00</td>
</tr>
<tr>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>12%</td>
<td>$140.00</td>
<td>$2,750</td>
<td>15%</td>
<td>$415</td>
<td>$2,295</td>
<td>$119.00</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED, TASK 2 - Not including travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$29,750</td>
<td>$136.00</td>
</tr>
<tr>
<td>TRAVEL</td>
<td>Total Task 2 - Including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$31,430</td>
<td>$136.00</td>
</tr>
<tr>
<td></td>
<td>Task 3: Recommend wireless technology options and design considerations</td>
<td>22</td>
<td>$170.00</td>
<td>$3,800</td>
<td>15%</td>
<td>$570</td>
<td>$3,230</td>
<td>$144.13</td>
</tr>
<tr>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>97.5</td>
<td>$160.00</td>
<td>$13,800</td>
<td>15%</td>
<td>$2,070</td>
<td>$11,730</td>
<td>$136.00</td>
</tr>
<tr>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>139.3</td>
<td>$140.00</td>
<td>$19,500</td>
<td>15%</td>
<td>$3,025</td>
<td>$16,475</td>
<td>$118.99</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED, TASK 3 - Not including travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$33,150</td>
<td></td>
</tr>
<tr>
<td>TRAVEL</td>
<td>Total Task 3 - Including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$34,830</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Task 4: Recommend a business model for deploying a wireless network</td>
<td>15.75</td>
<td>$170.00</td>
<td>$2,700</td>
<td>15%</td>
<td>$405</td>
<td>$2,295</td>
<td>$145.71</td>
</tr>
<tr>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>67.5</td>
<td>$160.00</td>
<td>$10,800</td>
<td>15%</td>
<td>$1,620</td>
<td>$9,180</td>
<td>$136.00</td>
</tr>
<tr>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>96.5</td>
<td>$140.00</td>
<td>$13,500</td>
<td>15%</td>
<td>$2,025</td>
<td>$11,475</td>
<td>$119.91</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED, TASK 4 - Not including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$22,950</td>
<td></td>
</tr>
<tr>
<td>TRAVEL</td>
<td>Total Task 4 - Including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$24,630</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Task 5: Present recommendations and prepare an RFP for design and implementation</td>
<td>20.6</td>
<td>$170.00</td>
<td>$3,500</td>
<td>15%</td>
<td>$525</td>
<td>$3,975</td>
<td>$144.42</td>
</tr>
<tr>
<td></td>
<td>Principal Engineer/Principal Analyst</td>
<td>87.5</td>
<td>$160.00</td>
<td>$14,000</td>
<td>15%</td>
<td>$2,100</td>
<td>$11,900</td>
<td>$136.00</td>
</tr>
<tr>
<td></td>
<td>Senior Engineer/Senior Analyst</td>
<td>125</td>
<td>$140.00</td>
<td>$17,500</td>
<td>15%</td>
<td>$2,625</td>
<td>$14,875</td>
<td>$119.00</td>
</tr>
<tr>
<td>TOTAL NOT TO EXCEED, TASK 5 - Not including travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$29,750</td>
<td></td>
</tr>
<tr>
<td>TRAVEL</td>
<td>Total Task 5 - Including Travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$31,430</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL NOT TO EXCEED (TASKS 1 – 5) PROFESSIONAL SERVICES - Not including travel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$123,250</td>
<td></td>
</tr>
<tr>
<td>TRAVEL</td>
<td>TOTAL TRAVEL (TASKS 1 – 5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$8,400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOTAL NOT TO EXCEED (TASKS 1 – 5) PROFESSIONAL SERVICES &amp; TRAVEL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$131,650</td>
<td></td>
</tr>
</tbody>
</table>

Consultant may reallocate funds among task and staff categories with advance notice and approval from City provided the total project cost is not exceeded.
EXHIBIT “D”
INSURANCE REQUIREMENTS

CONTRACTORS TO THE CITY OF PALO ALTO (CITY), AT THEIR SOLE EXPENSE, SHALL FOR THE TERM OF THE CONTRACT OBTAIN AND MAINTAIN INSURANCE IN THE AMOUNTS FOR THE COVERAGE SPECIFIED BELOW, AFFORDED BY COMPANIES WITH AM BEST’S KEY RATING OF A-VII, OR HIGHER, LICENSED OR AUTHORIZED TO TRANSACT INSURANCE BUSINESS IN THE STATE OF CALIFORNIA.

AWARD IS CONTINGENT ON COMPLIANCE WITH CITY’S INSURANCE REQUIREMENTS, AS SPECIFIED, BELOW:

<table>
<thead>
<tr>
<th>REQUIRED</th>
<th>TYPE OF COVERAGE</th>
<th>REQUIREMENT</th>
<th>MINIMUM LIMITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>WORKER’S COMPENSATION</td>
<td>STATUTORY</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>EMPLOYER’S LIABILITY</td>
<td>STATUTORY</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>GENERAL LIABILITY, INCLUDING PERSONAL INJURY, BROAD FORM PROPERTY DAMAGE BLANKET CONTRACTUAL, AND FIRE LEGAL LIABILITY</td>
<td>BODILY INJURY</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROPERTY DAMAGE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BODILY INJURY &amp; PROPERTY DAMAGE COMBINED</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>YES</td>
<td>AUTOMOBILE LIABILITY, INCLUDING ALL OWNED, HIRED, NON-OWNED</td>
<td>BODILY INJURY</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EACH PERSON</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- EACH OCCURRENCE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PROPERTY DAMAGE</td>
<td>$1,000,000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BODILY INJURY AND PROPERTY DAMAGE, COMBINED</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>YES</td>
<td>PROFESSIONAL LIABILITY, INCLUDING, ERRORS AND OMISSIONS, MALPRACTICE (WHEN APPLICABLE), AND NEGLIGENT PERFORMANCE</td>
<td>ALL DAMAGES</td>
<td>$1,000,000</td>
</tr>
</tbody>
</table>

THE CITY OF PALO ALTO IS TO BE NAMED AS AN ADDITIONAL INSURED: CONTRACTOR, AT ITS SOLE COST AND EXPENSE, SHALL OBTAIN AND MAINTAIN, IN FULL FORCE AND EFFECT THROUGHOUT THE ENTIRE TERM OF ANY RESULTANT AGREEMENT, THE INSURANCE COVERAGE HEREIN DESCRIBED, INSURING NOT ONLY CONTRACTOR AND ITS SUBCONSULTANTS, IF ANY, BUT ALSO, WITH THE EXCEPTION OF WORKERS’ COMPENSATION, EMPLOYER’S LIABILITY AND PROFESSIONAL INSURANCE, NAMING AS ADDITIONAL INSUREDS CITY, ITS COUNCIL MEMBERS, OFFICERS, AGENTS, AND EMPLOYEES.

I. INSURANCE COVERAGE MUST INCLUDE:
   A. A PROVISION FOR A WRITTEN THIRTY (30) DAY ADVANCE NOTICE TO CITY OF CHANGE IN COVERAGE OR OF COVERAGE CANCELLATION; AND
   B. A CONTRACTUAL LIABILITY ENDORSEMENT PROVIDING INSURANCE COVERAGE FOR CONTRACTOR’S AGREEMENT TO INDEMNIFY CITY.
   C. DEDUCTIBLE AMOUNTS IN EXCESS OF $5,000 REQUIRE CITY’S PRIOR APPROVAL.
II. CONTACTOR MUST SUBMIT CERTIFICATES(S) OF INSURANCE EVIDENCING REQUIRED COVERAGE.
III. ENDORSEMENT PROVISIONS, WITH RESPECT TO THE INSURANCE AFFORDED TO “ADDITIONAL INSUREDS”
   A. PRIMARY COVERAGE
   WITH RESPECT TO CLAIMS ARISING OUT OF THE OPERATIONS OF THE NAMED INSURED, INSURANCE AS AFFORDED BY THIS POLICY IS PRIMARY AND IS NOT ADDITIONAL TO OR CONTRIBUTING WITH ANY OTHER INSURANCE CARRIED BY OR FOR THE BENEFIT OF THE ADDITIONAL INSUREDS.
   B. CROSS LIABILITY
THE NAMING OF MORE THAN ONE PERSON, FIRM, OR CORPORATION AS INSUREDS UNDER THE POLICY SHALL NOT, FOR THAT REASON ALONE, EXTINGUISH ANY RIGHTS OF THE INSURED AGAINST ANOTHER, BUT THIS ENDORSEMENT, AND THE NAMING OF MULTIPLE INSUREDS, SHALL NOT INCREASE THE TOTAL LIABILITY OF THE COMPANY UNDER THIS POLICY.

C. NOTICE OF CANCELLATION

1. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR ANY REASON OTHER THAN THE NON-PAYMENT OF PREMIUM, THE ISSUING COMPANY SHALL PROVIDE CITY AT LEAST A THIRTY (30) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.

2. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR THE NON-PAYMENT OF PREMIUM, THE ISSUING COMPANY SHALL PROVIDE CITY AT LEAST A TEN (10) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.

NOTICES SHALL BE MAILED TO:

PURCHASING AND CONTRACT ADMINISTRATION
CITY OF PALO ALTO
P.O. BOX 10250
PALO ALTO, CA  94303
SOFTWARE AS A SERVICE SECURITY AND PRIVACY

TERMS AND CONDITIONS

This Exhibit shall be made a part of the City of Palo Alto’s Professional Services Agreement or any other contract entered into by and between the City of Palo Alto (the “City”) and ________________________________ (the “Consultant”) for the provision of Software as a Service to the City (the “Agreement”).

In order to assure the privacy and security of the personal information of the City’s customers and people who do business with the City, including, without limitation, vendors, utility customers, library patrons and other individuals and businesses, who are required to share such information with the City, as a condition of receiving services from the City or selling goods and services to the City, including, without limitation, the Software as a Service services provider (the “Consultant”) and its subcontractors, if any, including, without limitation, any Information Technology (“IT”) infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, described below, while it renders and performs the Services and furnishes goods, if any, described in the Statement of Work, Exhibit B, to the extent any scope of work implicates the confidentiality and privacy of the personal information of the City’s customers. The Consultant shall fulfill the data and information security requirements (the “Requirements”) set forth in Part A below.

A “secure IT environment” includes: (a) the IT infrastructure, by which the Services are provided to the City, including connection to the City’s IT systems; (b) the Consultant’s operations and maintenance processes needed to support the environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. “IT infrastructure” refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

In the event that, after the Effective Date, the Consultant reasonably determines that it cannot fulfill the Requirements, the Consultant shall promptly inform the City of its determination and submit, in writing, one or more alternate countermeasure options to the Requirements (the “Alternate Requirements” as set forth in Part B), which may be accepted or rejected in the reasonable satisfaction of the Information Security Manager (the “ISM”).

Part A. Requirements:

The Consultant shall at all times during the term of any contract between the City and the Consultant:

(a) Appoint or designate an employee, preferably an executive officer, as the security liaison to
the City with respect to the Services to be performed under this Agreement.

(b) Provide a full and complete response to the City’s Supplier Security and Privacy Assessment Questionnaire (the “Questionnaire”) to the ISM, and also report any major non-conformance to the Requirements, as and when requested. The response shall include a detailed implementation plan of required countermeasures, which the City requires the Consultant to adopt as countermeasures in the performance of the Services. In addition, as of the annual anniversary date of this Agreement the Consultant shall report to the City, in writing, any major changes to the IT infrastructure.

(c) Have adopted and implemented information security and privacy policies that are documented, are accessible to the City and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards. See the following:


(d) Conduct routine data and information security compliance training of its personnel that is appropriate to their role.

(e) Develop and maintain detailed documentation of the IT infrastructure, including software versions and patch levels.

(f) Develop an independently verifiable process, consistent with industry standards, for performing professional and criminal background checks of its employees that (1) would permit verification of employees’ personal identity and employment status, and (2) would enable the immediate denial of access to the City's confidential data and information by any of its employees who no longer would require access to that information or who are terminated.

(g) Provide a list of IT infrastructure components in order to verify whether the Consultant has met or has failed to meet any objective terms and conditions.

(h) Implement access accountability (identification and authentication) architecture and support role-base access control (“RBAC”) and segregation of duties (“SoD”) mechanisms for all personnel, systems and software used to provide the Services. “RBAC” refers to a computer systems security approach to restricting access only to authorized users. “SoD” is an approach that would require more than one individual to complete a security task in order to promote the detection and prevention of fraud and errors.

(i) Assist the City in undertaking annually an assessment to assure that: (1) all elements of the Services’ environment design and deployment are known to the City, and (2) it has implemented measures in accordance with industry best practices applicable to secure coding and secure IT architecture.

(j) Provide and maintain secure intersystem communication paths that would ensure the confidentiality, integrity and availability of the City's information.

(k) Deploy and maintain IT system upgrades, patches and configurations conforming to current patch and/or release levels by not later than one (1) week after its date of release. Emergency security patches must be installed within 24 hours after its date of release.

(l) Provide for the timely detection of, response to, and the reporting of security incidents, including on-going incident monitoring with logging.

(m) Notify the City within one (1) hour of detecting a security incident that results in the unauthorized access to or the misuse of the City's confidential data and information.
(n) Inform the City that any third party service provider(s) meet(s) all of the Requirements.
(o) Perform security self-audits on a regular basis and not less frequently than on a quarterly basis, and provide the required summary reports of those self-audits to the ISM on the annual anniversary date or any other date agreed to by the Parties.
(p) Accommodate, as practicable, and upon reasonable prior notice by the City, the City’s performance of random site security audits at the Consultant’s site(s), including the site(s) of a third party service provider(s), as applicable. The scope of these audits will extend to the Consultant’s and its third party service provider(s)’ awareness of security policies and practices, systems configurations, access authentication and authorization, and incident detection and response.
(q) Cooperate with the City to ensure that to the extent required by applicable laws, rules and regulations, the Confidential Information will be accessible only by the Consultant and any authorized third party service provider’s personnel.
(r) Perform regular, reliable secured backups of all data needed to maximize availability of the Services.
(s) Maintain records relating to the Services for a period of three (3) years after the expiration or earlier termination of this Agreement and in a mutually agreeable storage medium. Within thirty (30) days after the effective date of expiration or earlier termination of this Agreement, all of those records relating to the performance of the Services shall be provided to the ISM.
(t) Maintain the Confidential Information in accordance with applicable federal, state and local data and information privacy laws, rules and regulations.
(u) Encrypt the Confidential Information before delivering the same by electronic mail to the City and or any authorized recipient.
(v) Unless otherwise addressed in the Agreement, shall not hold the City liable for any direct, indirect or punitive damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the City’s IT environment, including, without limitation, IT infrastructure communications.

Part B. Alternate Requirements:
Vendor Information Security Assessment (VISA) Questionnaire

Purpose: This Vendor Information Security Assessment (VISA) Questionnaire requests information concerning a Cloud Service Provider (the Vendor), which intends to provide to the City of Palo Alto (the City) any or all of the following services: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS).

Note/Instructions:
- SaaS, PaaS and IaaS are each a ‘cloud’ servicing model, in which software and database applications, computer network infrastructure and/or computer hardware/software platforms is/are hosted by the Vendor and made available to customers interconnected in a network, typically the Internet.
- This Questionnaire is for the sole use of the intended Vendor and may contain confidential information of individuals and businesses collected, stored, and used the City. Any unauthorized collection, storage, use, review or distribution may be prohibited by California and/or Federal laws. If you are not the intended recipient of this Questionnaire, please contact the sender by e-mail and destroy all copies of the Questionnaire.
- The Vendor shall provide answers to the questions or information to the requests provided below.
- In the event that the Vendor determines that it cannot meet the City’s security and or privacy requirements, the Vendor may submit a request for an exception to the City’s requirements and propose alternative countermeasures to address the risks addressed in this Questionnaire. The City’s Information Security Manager (ISM) may approve or reject the exception request, depending on the risks associated with the exception request.

Security Exception Request shall be submitted if you cannot comply with this policy/requirements

A = Meets completely.
B = Partially meets. The Vendor may be required to provide additional requested information.
C = Doesn’t meet. The Vendor may be required to provide missing/additional detail.

Vendor Information:

<table>
<thead>
<tr>
<th>Vendor Organization Name</th>
<th>CTC Inc. Columbia Telecommunications Corporation d/b/a CTC Technology &amp; Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>10613 Concord Street, Kensington, MD 20895</td>
</tr>
<tr>
<td>Information Security Contact Person Name</td>
<td>Matthew DeHaven</td>
</tr>
<tr>
<td>City’s PM</td>
<td>Todd Henderson</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:mdehaven@ctcnet.us">mdehaven@ctcnet.us</a></td>
</tr>
<tr>
<td>Phone</td>
<td>301-933-1488</td>
</tr>
</tbody>
</table>
# 1.0 BUSINESS PROCESS AND DATA EXCHANGE REQUIREMENTS

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Please provide a detailed description of the Vendor’s business process that will be offered to the City, as this relates to the proposed requirements of the City’s RFP or other business requirements</td>
<td>CTC will provide fiber and wireless network design recommendations, strategic planning recommendations, business case analysis, and financial analysis of potential fiber optic and wireless network deployments. The business processes will involve the review and analysis of City infrastructure data, market research, and preparation of network design and business analysis materials.</td>
<td>C</td>
<td>Please provide requested detail</td>
</tr>
<tr>
<td>1.2</td>
<td>Has the Vendor adopted and implemented information security and privacy policies that are documented and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards or NIST 800-53 (National Institute of Standards – NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations)</td>
<td>CTC does not anticipate hosting any applications used by the City or requiring access to City IT resources. Although formal IT security audits are generally not requested by our clients for the type of consulting services we provide, we have in place best-practice security measures consistent with the risk management-based approach to threat mitigation defined by NIST SP 800-53.</td>
<td>A</td>
<td></td>
</tr>
</tbody>
</table>
### 1.3 What data exchange will occur between the City and the Vendor?

What data will be stored at the Vendor's or other third party's data storage location? (Provide data attributes with examples of the data to be stored)

**Example:** Payment Card Information, Social Security Number, Driving License number, Patron's Name, Address, Telephone etc.), which are examples of personal information, the privacy of which are protected by California constitutional and statutory law.

| A | We anticipate the data exchange will primarily be through e-mail, and as required due to file attachment size, via commercial “cloud”-based file sharing services (Google Docs, DropBox, etc.). We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materias (e.g. GIS data related to roadway attributes and other City infrastructure). |

### 1.4 In the event that the Vendor is required to store Private Information (PI), Personally Identifiable Information (PII), and Sensitive Information (SI) about individuals/organizations with the service provider’s business systems, how does the Vendor maintain the confidentiality of the information in accordance with applicable federal, state and local data and information privacy laws, rules and regulations? 

**CTC does not anticipate requiring access to or storing PI, PII, or SI about individuals/organizations. In rare cases when this has been required in the past, CTC has conducted formal IT security audits compliant with client standards, and has successfully implemented risk mitigation plans consistent with these standards.**

<p>| A | |
| 1.5 | What mechanism and/or what types of tool(s) will be used to exchange data between the City and The Vendor? <em>Example: (VPN, Data Link, Frame Relay, HTTP, HTTPS, FTP, FTPS, etc.)</em> | We anticipate primarily transfer of data through email exchange. CTC does not anticipate requiring access to or transmitting PI, PII, or SI about individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materials (e.g. GIS data related to roadway attributes and other City physical infrastructure). Information provided to the City will include conceptual fiber network designs and financial analysis that we expect will be made publically available upon completion. | C |
| 1.6 | What types of data storage (work in progress storage and backup storage) are present or will be | CTC does not anticipate requiring access to or storing PI, PII, or SI about | A |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **1.7** | Is e-mail integration required between the City and the Vendor?  
*Example: The provision of services may require the City to provide the Vendor with an e-mail account on the City’s e-mail server.* |   | CTC does not require integration with the city’s email.  
A |
| **1.8** | Has the Vendor ever been subjected to either an electronic or physical security breach? Please describe the event(s) and the steps taken to mitigate the breach(es).  
What damages or exposure resulted? Are records of breaches and issues maintained and will these records be available for inspection by the City? | No. | NA |
| **1.9** | Does the Vendor maintain formal security policies and procedures to comply with applicable statutory or industry practice requirements/standards? Are records maintained to demonstrate compliance or certification? Does the Vendor allow client audit of these records? Note: Please submit supporting documentation. | Formal policies are implemented within CTC’s IT infrastructure related to electronic access controls. Statutory and/or industry compliance policies are implemented as-needed on a project basis.  
A |
| **2.0** | What are the internet and the browser security configurations for the cloud application? What security | N/A | NA |
standards and requirements does the Vendor maintain to ensure application security at the user interface? (A set of detailed documentation should be provided to support the compliance).

<table>
<thead>
<tr>
<th>2.0 APPLICATION/SOLUTION CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>#</strong></td>
</tr>
<tr>
<td>2.1</td>
</tr>
<tr>
<td>2.2</td>
</tr>
<tr>
<td>2.3</td>
</tr>
<tr>
<td>Question</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2.4 What is the Vendor's application(s) hosting hardware and software platform? Provide a detailed description, including security patches or security applications in use. Example: Windows or Unix Operating System (OS) and other detail.</td>
</tr>
<tr>
<td>2.5 How does the Vendor's application and database architecture to manage or promote segregation of the City's data (related to its function as a local government agency) from the data of individuals providing services to or receiving services from the City?</td>
</tr>
<tr>
<td>2.6 Describe the Vendor's server and network infrastructure. Please provide server and network infrastructure deployment topology, including data flow architecture, including but not limited to security management applications, firewalls, etc.</td>
</tr>
</tbody>
</table>
2.7 Please provide a detail proposed solution that will be developed as a part of the Vendor’s implementation to support this project. (For example detailed solution architecture, secured data flow to support business processes, etc.).

<table>
<thead>
<tr>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.0 DATA PROTECTION

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>What will be the medium of data exchange between the City and Vendor?</td>
<td>Primarily email.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>How will the data be kept secure during the data exchange process? Example: (VPN, Data Link, Frame Relay, HTTP, HTTPS, FTP, FTPS, etc.)</td>
<td>CTC does not anticipate requiring access to or transferring PI, PII, or SI about individuals/organizations. CTC is open to using any preferred transfer solution or technology as deemed appropriate by the City.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>How will the City’s data be kept physically and logically secure at the Vendor’s preferred storage location? Example: Locked storage, Digitally, Encrypted etc.</td>
<td>Work materials in progress will be stored on CTC’s internal servers, secured within its headquarters location. The site utilizes electronic keycard access to all doorways, and is protected by an actively monitored electronic security surveillance system. CTC has a formal, documented physical access policy requiring</td>
<td>C</td>
<td>What data transfer is required? Please advise.</td>
</tr>
</tbody>
</table>
logging and escort of all non-staff visitors. Only CTC staff have electronic credentials to access internal storage servers. No direct external (Internet-based) access to our servers is allowed without VPN access.

We anticipate primarily transfer of data through email exchange. CTC does not anticipate requiring access to or transmitting PI, PII, or SI about individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materiais (e.g. GIS data related to roadway attributes and other City physical infrastructure). Information provided to the City will include conceptual fiber network designs and financial analysis that we expect will be made publically available upon completion.

### 3.4 What application level protections are in place to prevent the Vendor’s or a subcontractor/third party’s staff member from viewing unauthorized confidential information? For example, encryption, masking, etc.

CTC does not anticipate requiring access to or storing PI, PII, or SI about individuals/organizations. We anticipate data exchange requirements will be limited to publically accessible information and other generally non-sensitive materiais (e.g. GIS data related to roadway attributes and other City infrastructure).

| A |

### 3.5 What controls does the Vendor exercise over the qualification and performance of its team? Of their subcontractor/third party’s team(s)? (For example, criminal background

Our team members undergo a background check and a strict qualification interview that follows closely with the Top Grading interview technique. Qualifications are determined by role/labor

<p>| a |</p>
<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response</th>
<th>Score</th>
<th>COPA’s Security Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>What are the Vendor’s method(s) used to keep data secured during the data backup process?</td>
<td>Offsite data backups are transferred over an AES 256-bit encrypted VPN tunnel.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Is the Vendor’s encryption technology used to encrypt whole or selective data?</td>
<td>All data is encrypted during offsite backup transfer.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>What types of storage media will the Vendor use for data backup purposes? For example, Tape, Hard Disk Drive or any other devices.</td>
<td>Hard Disk Drive.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Are the Vendor’s backup storage devices encrypted? If 'yes,' please provide encryption specification, with type of encryption algorithm and detail process of encryption handling. If 'no,' provide a detailed description.</td>
<td>No, data is not encrypted on storage devices. Offsite data backups are transferred over an AES 256-bit encrypted VPN tunnel. No physical transport of storage media occurs for backups.</td>
<td>B</td>
<td>Depending upon the vendor’s response of the type of data processed we’ll decide the data encryption requirements</td>
</tr>
</tbody>
</table>
(with processes, tools and technology) to keep data secured during the back-up process.

## 5.0 DATA RETENTION

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>What is the Vendor’s standard data retention period of the backed up data? The data retention process shall comply with the City’s data 7 (seven) years data retention policy. Note: In the event that the Vendor cannot comply with this requirement then the City’s Project Manager shall approval from the City’s data retention schedule/policy owner.</td>
<td>7 years.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>Are the data backup storage media at the Vendor’s location or other third party location?</td>
<td>All backups are stored at a CTC regional location.</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>If the Vendor’s backup storage devices are stored with another company, please</td>
<td>N/A</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5.5</strong></td>
<td><strong>What is the media transfer process (i.e. The lock box process used to send tapes off-site)?</strong></td>
<td>Data storage devices are not physically transported. Offsite data backup occurs between CTC locations over AES 256-bit encrypted VPN tunnels.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5.6</strong></td>
<td><strong>Who has access to the data storage media lockbox(es)? (Provide Name and Role)</strong></td>
<td>Only CTC IT Administrators (Matthew DeHaven, CIO/CISO and Eric Wirth, Deputy CIO/CISO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5.7</strong></td>
<td><strong>Who on the Vendor’s staff or subcontractor/third party’s staff is/are authorized to access backup data storage media? (Provide Name and Role)</strong></td>
<td>Only CTC IT Administrators (Matthew DeHaven, CIO/CISO and Eric Wirth, Deputy CIO/CISO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5.8</strong></td>
<td><strong>What is the backup data storage media receipt and release authorization process(es)? (Please submit a soft copy of the process)</strong></td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 6.0 ACCOUNT PROVISIONING AND DE-PROVISIONING
(The Vendor must receive formal pre-authorization from the City’s Information Security Manager prior to provisioning and de-provisioning of application access account.)
<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional Information/Clarification Required from the Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>What is the account provisioning/removal process? Example: how are users accounts created and managed?)</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.2</td>
<td>What is the account deprovisioning/removal process? Example: how are users accounts created and managed?)</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.3</td>
<td>How will the City’s employees gain access to required application(s)?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>6.4</td>
<td>Does the application(s) have the capability to restrict access only from the City’s WAN (Wide Area Network)?</td>
<td>N/A</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### 7.0 PASSWORD MANAGEMENT

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Response from the Vendor</th>
<th>Score</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Information/Clarification Required from the Vendor</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>7.1</td>
<td>What will be the policy and/or procedures for the logging, authentication, authorization and password management scheme? (Please provide a soft copy of the process)</td>
<td>City employees will not require access to any applications hosted or developed by CTC.</td>
<td>C</td>
<td>Please confirm that the City’s employees don’t need to access CTC’s application.</td>
</tr>
<tr>
<td>7.2</td>
<td>Where will the login and password credentials be stored?</td>
<td>N/A</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>7.3</td>
<td>Are the password credentials stored with encryption? If ‘yes,’ please provide encryption scheme detail.</td>
<td>N/A</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>
| 7.4 | The Vendor’s application must comply with the following password requirements. Does the Vendor’s application meet these requirements? | N/A | NA | 1. First time password must be unique to an individual and require the user to change it upon initial login.  
2. If the password is sent via plain text email to the City employee to mitigate security |
3. The City requires first time password to have a time-out capability of no more than 7 days.

4. The e-mail notification must not be copied to anyone except the user.

5. The permanent/long term password must be changed frequently (at least TWICE a year)

6. E-mail notification must be sent to the user whenever the password has been updated.

7. User should not be able to view data or conduct business unless an initial password has been updated with a different password.

8. The Vendor shall inform the City’s users that, when a new password is created, the user shall not use the City’s LDAP (Lightweight Directory Access Control) exposure.
<table>
<thead>
<tr>
<th>Protocol) password.</th>
<th>9. The password must have 8 or more alphanumerical (/) characters and it must contain at least one character from each of the bullets noted below (i.e. Each line shall contribute at least one character):</th>
</tr>
</thead>
<tbody>
<tr>
<td>• abcdefghijklmnopqrstuvwxyz</td>
<td>• ABCDEFGHIJKLMNOPQRSTUVWXYZ</td>
</tr>
<tr>
<td>• 0123456789</td>
<td>• !@$%^&amp;*()-+=~&gt;,&lt;&quot;'?;:[{}]</td>
</tr>
</tbody>
</table>

End Of Document
Information Privacy Policy

Release and Version: 1st Release, Version 2.2
Release Date: 31 January, 2013
Document Classification: Need to Know
CONTENTS

DOCUMENT CONTROLS ............................................................................................................................ 2
CHANGE RECORD ......................................................................................................................................... 2
APPROVAL .................................................................................................................................................. 2
DISTRIBUTION ............................................................................................................................................ 2

1. OBJECTIVE ........................................................................................................................................... 3
   A) INTENT ............................................................................................................................................... 3
   B) SCOPE ............................................................................................................................................... 3
   C) CONSEQUENCES ............................................................................................................................... 3
   D) EXCEPTIONS ....................................................................................................................................... 3
   E) MUNICIPAL ORDINANCE .................................................................................................................. 4

2. RESPONSIBILITIES OF CITY STAFF .................................................................................................... 4
   A) RESPONSIBILITY OF CIO AND ISM ............................................................................................... 4
   B) RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE .................................. 4
   C) RESPONSIBILITY OF USERS .......................................................................................................... 4
   D) RESPONSIBILITY OF INFORMATION TECHNOLOGY (IT) MANAGERS ..................................... 5
   E) RESPONSIBILITY OF AUTHORIZATION COORDINATION ............................................................ 5

3. PRIVACY POLICY .................................................................................................................................... 5
   A) OVERVIEW ......................................................................................................................................... 5
   B) PERSONAL INFORMATION AND CHOICE .................................................................................... 5
   C) METHODS OF COLLECTION OF PERSONAL INFORMATION ..................................................... 5
   D) UTILITIES SERVICE .......................................................................................................................... 6
   E) PUBLIC DISCLOSURE ......................................................................................................................... 6
   F) ACCESS TO PERSONAL INFORMATION ......................................................................................... 6
   G) SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE .............................................................. 6
   H) DATA RETENTION / INFORMATION RETENTION ......................................................................... 7
   I) SOFTWARE AS A SERVICE (SaaS) OVERSIGHT ............................................................................ 7
   J) FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003 (FACT) ........................................ 7

4. CONTACTS .............................................................................................................................................. 8
DOCUMENT CONTROLS

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Information Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>City of Palo Alto Website and SharePoint</td>
</tr>
<tr>
<td>Document Author</td>
<td>Raj Patel</td>
</tr>
<tr>
<td>Document Manager</td>
<td>Raj Patel</td>
</tr>
<tr>
<td>Contributors</td>
<td>Jonathan Reichental, Shiva Swaminathan, Tom Auzenne, Joe Blackwell, Grant Kolling</td>
</tr>
</tbody>
</table>

CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Jul-12</td>
<td>Raj Patel</td>
<td>0.01</td>
<td>First draft developed</td>
</tr>
<tr>
<td>26-Sep-12</td>
<td>Raj Patel</td>
<td>1.0</td>
<td>First draft released for review</td>
</tr>
<tr>
<td>09-Nov-12</td>
<td>Raj Patel</td>
<td>1.5</td>
<td>Updated first draft for review</td>
</tr>
<tr>
<td>19-Nov-12</td>
<td>Raj Patel</td>
<td>1.6</td>
<td>Additional updates as identified</td>
</tr>
<tr>
<td>22-Nov-12</td>
<td>Raj Patel</td>
<td>1.7</td>
<td>Revised table of content</td>
</tr>
<tr>
<td>26-Nov-12</td>
<td>Raj Patel</td>
<td>1.8</td>
<td>Revised followed by review from Jonathan Reichental and Tom Auzenne</td>
</tr>
<tr>
<td>06-Dec-12</td>
<td>Raj Patel</td>
<td>1.92</td>
<td>Revised according to comments from Jonathan Reichental</td>
</tr>
<tr>
<td>14-Jan-13</td>
<td>Raj Patel</td>
<td>2.0</td>
<td>Revised according to comments from Grant Kolling</td>
</tr>
<tr>
<td>31-Jan-13</td>
<td>Raj Patel</td>
<td>2.2</td>
<td>Revised according to recommendations from Information Security Steering Committee</td>
</tr>
</tbody>
</table>

APPROVAL

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Role</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>06-Dec-12</td>
<td>Raj Patel</td>
<td>Information Security Manager; Information Technology Department</td>
<td>Approved</td>
</tr>
<tr>
<td>06-Dec-12</td>
<td>Jonathan Reichental</td>
<td>CIO; Information Technology Department</td>
<td>Approved</td>
</tr>
<tr>
<td>06-Dec-12</td>
<td>Tom Auzenne</td>
<td>Assistant Director, Utilities Department</td>
<td>Approved</td>
</tr>
<tr>
<td>14-Jan-13</td>
<td>Grant Kolling</td>
<td>Senior Assistant City Attorney; City Attorney’s Office</td>
<td>Approved</td>
</tr>
<tr>
<td>14-Jan-13</td>
<td>Information Security Steering Committee</td>
<td>Sponsor</td>
<td>Approved</td>
</tr>
</tbody>
</table>

DISTRIBUTION

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>City of Palo Alto Employees, Service Providers, Residents and Businesses</td>
<td>City of Palo Alto Website and SharePoint</td>
</tr>
</tbody>
</table>
1. Objective

The City of Palo Alto (the “City”) strives to promote and sustain a superior quality of life for persons in Palo Alto. In promoting the quality of life of these persons, it is the policy of the City, consistent with the provisions of the California Public Records Act, California Government Code §§ 6250 – 6270, to take appropriate measures to safeguard the security and privacy of the personal (including, without limitation, financial) information of persons, collected in the ordinary course and scope of conducting the City’s business as a local government agency. These measures are generally observed by federal, state and local authorities and reflected in federal and California laws, the City’s rules and regulations, and industry best practices, including, without limitation, the provisions of California Civil Code §§ 1798.3(a), 1798.24, 1798.79.8(b), 1798.80(e), 1798.81.5, 1798.82(e), 1798.83(e)(7), and 1798.92(c). Though some of these provisions do not apply to local government agencies like the City, the City will conduct business in a manner which promotes the privacy of personal information, as reflected in federal and California laws. The objective of this Policy is to describe the City’s data security goals and objectives, to ensure the ongoing protection of the Personal Information, Personally Identifiable Information, Protected Critical Infrastructure Information and Personally Identifying Information of persons doing business with the City and receiving services from the City or a third party under contract to the City to provide services. The terms “Personal Information,” “Protected Critical Infrastructure Information”, “Personally Identifiable Information” and “Personally Identifying Information” (collectively, the “Information”) are defined in the California Civil Code sections, referred to above, and are incorporated in this Policy by reference.

A) INTENT

The City, acting in its governmental and proprietary capacities, collects the Information pertaining to persons who do business with or receive services from the City. The Information is collected by a variety of means, including, without limitation, from persons applying to receive services provided by the City, persons accessing the City’s website, and persons who access other information portals maintained by the City’s staff and/or authorized third-party contractors. The City is committed to protecting the privacy and security of the Information collected by the City. The City acknowledges federal and California laws, policies, rules, regulations and procedures, and industry best practices are dedicated to ensuring the Information is collected, stored and utilized in compliance with applicable laws.

The goals and objectives of the Policy are: (a) a safe, productive, and offensive work environment for all users having access to the City’s applications and databases; (b) the appropriate maintenance and security of database information assets owned by, or entrusted to, the City; (c) the controlled access and security of the Information provided to the City’s staff and third party contractors; and (d) faithful compliance with legal and regulatory requirements.

B) SCOPE

The Policy will guide the City’s staff and, indirectly, third party contractors, which are by contract required to protect the confidentiality and privacy of the Information of the persons whose personal information data are intended to be covered by the Policy and which will be advised by City staff to conform their performances to the Policy should they enjoy conditional access to that information.

C) CONSEQUENCES

The City’s employees shall comply with the Policy in the execution of their official duties to the extent their work implicates access to the Information referred to in this Policy. A failure to comply may result in
employment and/or legal consequences.

D) EXCEPTIONS

In the event that a City employee cannot fully comply with one or more element(s) described in this Policy, the employee may request an exception by submitting Security Exception Request. The exception request will be reviewed and administered by the City’s Information Security Manager (the “ISM”). The employee, with the approval of his or her supervisor, will provide any additional information as may be requested by the ISM. The ISM will conduct a risk assessment of the requested exception in accordance with guidelines approved by the City’s Chief Information Officer (“CIO”) and approved as to form by the City Attorney. The Policy’s guidelines will include at a minimum: purpose, source, collection, storage, access, retention, usage, and protection of the Information identified in the request. The ISM will consult with the CIO to approve or deny the exception request. After due consideration is given to the request, the exception request disposition will be communicated, in writing, to the City employee and his or her supervisor. The approval of any request may be subject to countermeasures established by the CIO, acting by the ISM.

E) MUNICIPAL ORDINANCE

This Policy will supersede any City policy, rule, regulation or procedure regarding information privacy.

2. RESPONSIBILITIES OF CITY STAFF

A) RESPONSIBILITY OF CIO AND ISM

The CIO, acting by the ISM, will establish an information security management framework to initiate and coordinate the implementation of information security measures by the City’s government.

The City’s employees, in particular, software application users and database users, and, indirectly, third party contractors under contract to the City to provide services, shall by guided by this Policy in the performance of their job responsibilities.

The ISM will be responsible for: (a) developing and updating the Policy, (b) enforcing compliance with and the effectiveness of the Policy; (c) the development of privacy standards that will manifest the Policy in detailed, auditable technical requirements, which will be designed and maintained by the persons responsible for the City’s IT environments; (d) assisting the City’s staff in evaluating security and privacy incidents that arise in regard to potential violations of the Policy; (e) reviewing and approving department-specific policies and procedures which fall under the purview of this Policy; and (f) reviewing Non-Disclosure Agreements (NDAs) signed by third party contractors, which will provide services, including, without limitation, local or ‘cloud-based’ software services to the City.

B) RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE

The Information Security Steering Committee (the “ISSC”), which is comprised of the City’s employees, drawn from the various City departments, will provide the primary direction, prioritization and approval for all information security efforts, including key information security and privacy risks, programs, initiatives and activities. The ISSC will provide input to the information security and privacy strategic planning processes to ensure that information security risks are adequately considered, assessed and addressed at the appropriate City department level.
C) RESPONSIBILITY OF USERS

All authorized users of the Information will be responsible for complying with information privacy processes and technologies within the scope of responsibility of each user.

D) RESPONSIBILITY OF INFORMATION TECHNOLOGY (IT) MANAGERS

The City’s IT Managers, who are responsible for internal, external, direct and indirect connections to the City’s networks, will be responsible for configuring, maintaining and securing the City’s IT networks in compliance with the City’s information security and privacy policies. They are also responsible for timely internal reporting of events that may have compromised network, system or data security.

E) RESPONSIBILITY OF AUTHORIZATION COORDINATION

The ISM will ensure that the City’s employees secure the execution of Non-Disclosure Agreements (NDA), whenever access to the Information will be granted to third party contractors, in conjunction with the Software as a Service (SaaS) Security and Privacy Terms and Conditions. An NDA must be executed prior to the sharing of the Information of persons covered by this Policy with third party contractors. The City’s approach to managing information security and its implementation (i.e. objectives, policies, processes, and procedures for information security) will be reviewed independently by the ISM at planned intervals, or whenever significant changes to security implementation have occurred.

The CIO, acting by the ISM, will review and recommend changes to the Policy annually, or as appropriate, commencing from the date of its adoption.

3. PRIVACY POLICY

A) OVERVIEW

The Policy applies to activities that involve the use of the City’s information assets, namely, the Information of persons doing business with the City or receiving services from the City, which are owned by, or entrusted to, the City and will be made available to the City’s employees and third party contractors under contract to the City to provide Software as a Service consulting services. These activities include, without limitation, accessing the Internet, using e-mail, accessing the City’s intranet or other networks, systems, or devices.

The term “information assets” also includes the personal information of the City’s employees and any other related organizations while those assets are under the City’s control. Security measures will be designed, implemented, and maintained to ensure that only authorized persons will enjoy access to the information assets. The City’s staff will act to protect its information assets from theft, damage, loss, compromise, and inappropriate disclosure or alteration. The City will plan, design, implement and maintain information management systems, networks and processes in order to assure the appropriate confidentiality, integrity, and availability of its information assets to the City’s employees and authorized third parties.

B) PERSONAL INFORMATION AND CHOICE

Except as permitted or provided by applicable laws, the City will not share the Information of any person doing business with the City, or receiving services from the City, in violation of this Policy, unless that person has consented to the City’s sharing of such information during the conduct of the City’s business as a local government agency with third parties under contract to the City to provide services.
C) METHODS OF COLLECTION OF PERSONAL INFORMATION

The City may gather the Information from a variety of sources and resources, provided that the collection of such information is both necessary and appropriate in order for the City to conduct business as a local government agency in its governmental and proprietary capacities. That information may be gathered at service windows and contact centers as well as at web sites, by mobile applications, and with other technologies, wherever the City may interact with persons who need to share such information in order to secure the City's services.

The City's staff will inform the persons whose Information are covered by this Policy that the City's web site may use "cookies" to customize the browsing experience with the City of Palo Alto web site. The City will note that a cookie contains unique information that a web site can use to track, among others, the Internet Protocol address of the computer used to access the City's web sites, the identification of the browser software and operating systems used, the date and time a user accessed the site, and the Internet address of the website from which the user linked to the City's web sites. Cookies created on the user's computer by using the City's web site do not contain the Information, and thus do not compromise the user's privacy or security. Users can refuse the cookies or delete the cookie files from their computers by using any of the widely available methods. If the user chooses not to accept a cookie on his or her computer, it will not prevent or prohibit the user from gaining access to or using the City's sites.

D) UTILITIES SERVICE

In the provision of utility services to persons located within Palo Alto, the City of Palo Alto Utilities Department ("CPAU") will collect the Information in order to initiate and manage utility services to customers. To the extent the management of that information is not specifically addressed in the Utilities Rules and Regulations or other ordinances, rules, regulations or procedures, this Policy will apply; provided, however, any such Rules and Regulations must conform to this Policy, unless otherwise directed or approved by the Council. This includes the sharing of CPAU-collected Information with other City departments except as may be required by law.

Businesses and residents with standard utility meters and/or having non-metered monthly services will have secure access through a CPAU website to their Information, including, without limitation, their monthly utility usage and billing data. In addition to their regular monthly utilities billing, businesses and residents with non-standard or experimental electric, water or natural gas meters may have their usage and/or billing data provided to them through non-City electronic portals at different intervals than with the standard monthly billing.

Businesses and residents with such non-standard or experimental metering will have their Information covered by the same privacy protections and personal information exchange rules applicable to Information under applicable federal and California laws.

E) PUBLIC DISCLOSURE

The Information that is collected by the City in the ordinary course and scope of conducting its business could be incorporated in a public record that may be subject to inspection and copying by the public, unless such information is exempt from disclosure to the public by California law.

F) ACCESS TO PERSONAL INFORMATION

The City will take reasonable steps to verify a person’s identity before the City will grant anyone online access to that person’s Information. Each City department that collects Information will afford access to affected persons who can review and update that information at reasonable times.
G) SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE

Except as otherwise provided by applicable law or this Policy, the City will treat the Information of persons covered by this Policy as confidential and will not disclose it, or permit it to be disclosed, to third parties without the express written consent of the person affected. The City will develop and maintain reasonable controls that are designed to protect the confidentiality and security of the Information of persons covered by this Policy.

The City may authorize the City’s employee and or third party contractors to access and/or use the Information of persons who do business with the City or receive services from the City. In those instances, the City will require the City’s employee and/or the third party contractors to agree to use such Information only in furtherance of City-related business and in accordance with the Policy.

If the City becomes aware of a breach, or has reasonable grounds to believe that a security breach has occurred, with respect to the Information of a person, the City will notify the affected person of such breach in accordance with applicable laws. The notice of breach will include the date(s) or estimated date(s) of the known or suspected breach, the nature of the Information that is the subject of the breach, and the proposed action to be taken or the responsive action taken by the City.

H) DATA RETENTION / INFORMATION RETENTION

The City will store and secure all Information for a period of time as may be required by law, or if no period is established by law, for seven (7) years, and thereafter such information will be scheduled for destruction.

I) SOFTWARE AS A SERVICE (SaaS) OVERSIGHT

The City may engage third party contractors and vendors to provide software application and database services, commonly known as Software-as-a-Service (SaaS).

In order to assure the privacy and security of the Information of those who do business with the City and those who received services from the City, as a condition of selling goods and/or services to the City, the SaaS services provider and its subcontractors, if any, including any IT infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, while it performs such services and/or furnishes goods to the City, to the extent any scope of work or services implicates the confidentiality and privacy of the Information.

These requirements include information security directives pertaining to: (a) the IT infrastructure, by which the services are provided to the City, including connection to the City’s IT systems; (b) the SaaS services provider’s operations and maintenance processes needed to support the IT environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. The term “IT infrastructure” refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

Prior to entering into an agreement to provide services to the City, the City’s staff will require the SaaS services provider to complete and submit an Information Security and Privacy Questionnaire. In the event that the SaaS services provider reasonably determines that it cannot fulfill the information security requirements during the course of providing services, the City will require the SaaS services provider to promptly inform the ISM.

J) FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003

CPAU will require utility customers to provide their Information in order for the City to initiate and manage utility services to them.
Federal regulations, implementing the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), including the Red Flag Rules, require that CPAU, as a “covered financial institution or creditor” which provides services in advance of payment and which can affect consumer credit, develop and implement procedures for an identity theft program for new and existing accounts to detect, prevent, respond and mitigate potential identity theft of its customers’ Information.

CPAU procedures for potential identity theft will be reviewed independently by the ISM annually or whenever significant changes to security implementation have occurred. The ISM will recommend changes to CPAU identity theft procedures, or as appropriate, so as to conform to this Policy.

There are California laws which are applicable to identity theft; they are set forth in California Civil Code § 1798.92.

4. CONTACTS

Information Security Manager: Patel, Raj <Raj.Patel@CityofPaloAlto.org>
Chief Information Officer: Reichental, Jonathan <Jonathan.Reichental@CityofPaloAlto.org>
Utilities Department: Auzenne, Tom <Tom.Auzenne@CityofPaloAlto.org>
City Attorney’s Office: Kolling, Grant <Grant.Kolling@CityofPaloAlto.org>