Park City Municipal Corporation

REQUEST FOR PROPOSALS (NON-BID) FOR

HRIS & Payroll Software

NOTICE
REQUEST FOR PROPOSALS (NON-BID)
HRIS & Payroll Software

PROPOSALS DUE: Thursday, October 12, 2017 5:00 p.m. MST

PROJECT NAME: HRIS & Payroll Software

RFP AVAILABLE: Thursday, September 21, 2017

PROJECT LOCATION: City Hall, 445 Marsac Avenue, Park City, UT 84060

PROJECT DESCRIPTION: Park City Municipal Corporation ("PCMC") requests proposals from qualified firms for software to be used as part of the human resources and payroll processes.

PROJECT DEADLINE: Thursday, November 23, 2017 5:00 p.m. MST

OWNER: Park City Municipal Corporation
P.O. Box 1480
Park City, UT 84060

CONTACT: *Brooke Moss, HR Manager*
bmoss@parkcity.org
fax: 435-615-4902
All questions shall be submitted in writing via email to Brooke Moss no later than Tuesday, October 10, 2017 5:00 p.m. MST.

Park City reserves the right to reject any or all proposals received. Furthermore, the City shall have the right to waive any informality or technicality in proposals received when in the best interest of the City.

I. Introduction

PCMC requests proposals from qualified firms for software to be used as part of the human resources and payroll processes.

II. Scope of Project

The software should include an easy-to use and aesthetically pleasing interface (dashboard) and the following modules are required for response: Payroll, Human Resources, Employee self-service, timekeeping, recruiting and onboarding. This project is to replace the current HR and Payroll (HRIS) software used at the City with an integrated product that works smoothly between modules. Must be able to transition payroll information to current City Financial software Eden. Installation, transfer of data from old system, ongoing updates, maintenance, and technical support will also be expected.

III. Content of Proposal

Interested firms shall provide a PDF electronic version of their proposal. **Proposals should be 35 pages or less** (not including the cover page and appendix items) and include the following information:

1. Cover Page:
    a. Name, address, email, and website of the company.

2. Narrative of the Firm's Qualifications and Relevant Experience:
    a. Year founded.
    b. How many employees in your company are full time?
    c. Brief history of your company.
    d. What is your primary business focus?
    e. What is your target market?
    f. How many years has the system you are offering been released?
    g. How many HRIS and payroll clients do you have?
    h. What is the average size of your clients?
    i. What are your company's annual sales and revenues?
    j. Provide a short description of your company's disaster recovery options.
    k. Who are your technical partners?
    l. Please provide 3 references. Government organizations preferred.

3. Cost Proposal
    a. Cost proposal shall include all costs incurred by the submitter during the installation, start-up, and warranty periods. Park City currently employs 849 employees. Only 280 would access an employee self-service portal if available.
    b. Cost proposal must be itemized and include, at a minimum, the above mentioned categories in addition to detailed costs for materials involved.
    c. Cost proposal MAY include a discount given for occasional workers who receive no more than 2 paychecks per year. Park City employs approximately 200 of these employees.
    d. Cost proposal should include any discount that would be given for collaborative work or marketing/branding opportunities.

e. If there is a conflict between the written and numerical cost amounts, the written amount shall supersede.

4. Product Overview (please answer the following questions). Please provide only brief answers. More detailed information will be requested at a later date from vendors who meet module and price considerations.
    a. Does the software provide all of the following services/modules:
        i. Payroll
        ii. Human Resources
        iii. Recruiting
        iv. Onboarding
        v. Timekeeping
        vi. Employee self service
    b. Please provide a brief description of your recruiting and applicant tracking system.
        i. What job boards are supported in your product?
        ii. What background check organizations are supported in your product?
    c. How is a rehire identified in applicant tracking?
    d. Describe your employer configurable new hire workflow.
    e. Describe your employer termination workflow.
    f. Describe your onboarding solution.
    g. Describe your HR system.
    h. As regulations change, how do you ensure your clients stay in compliance?
    i. Describe your key compensation features of the system.
    j. What types of reports are available for compensation?
    k. Describe how your system manages bonus and/or discretionary pay.
    l. Describe how your system manages separation pay.
    m. Explain how pay changes are entered into the system.
    n. Describe how salary range/grade changes are made in the system.
    o. Please describe your capabilities to track employee discipline and grievances.
    p. Describe the integration between benefits and payroll.
    q. Describe benefits administration in your system.
    r. Describe the system for online benefits enrollment.
    s. Describe how this solution helps the employees navigate through benefits enrollment.
    t. How does FMLA management work?
    u. How does your system recognize FMLA time? How does it coordinate disability leave and FMLA?
    v. List which modules experience down time when payroll is processing.
    w. Describe how adjustments to exempt salaries are calculated when they are partial payments only.
    x. Describe how and how many years of existing employee history is extracted and imported to your system at conversion.
    y. Is it possible to purchase additional years of employee compensation history? We are required by State law, due to the State pension system, to maintain reportable payroll data for 60 years after an employee leaves employment. Can you facilitate this? What would be the charge for each additional year?
    z. Describe your application's employee self-service functionality. What are the major features?
    aa. Are managers able to access their employee's info in the system? If so, what , iinformation is available to them?

bb. Does the system provide customized reporting?
cc. Describe the delivered tools and methods required to customize your application. Who has to perform each customization, the vendor or the City?
dd. Provide an overview of your customer support and maintenance services.
ee. What hours does your company provide support? Is there an after-hours emergency contact if needed?
ff. How often do you release new versions of your software? Would we receive change information prior to release?
gg. How do you determine and prioritize changes in your system?
hh. What ongoing training is available for administrative users?
ii. What is the process for effectively managing the implementation process?
jj. Please provide a typical implementation timeline and calendar.
kk. Is there a primary point of contact for implementation?
ll. Describe your approach to identifying, managing, mitigating and tracking of project risks.
mm. During implementation, do you assist with process improvement and/or best practices?
nn. What is your process for moving from implementation to customer maintenance?
oo. Explain if you cannot meet the technical and security requirements listed in Exhibit C of the Contract

4. Insurance

A statement indicating that the firm will provide the required insurance. The chosen firm will be expected to provide the City with a certificate of insurance. Please see the Service Provider Agreement, included as Attachment A, for all relevant insurance requirements.

Vendors may submit any questions they have about the City or the above information as of 5:00 p.m. MST on Tuesday, October 10, 2017. Please allow at least 24 hours to receive a response. Responses will be posted on our website.

Park City Municipal Corporation reserves the right to cancel or modify the terms of this RFP and/or the project at any time and for any reason preceding contract award and reserves the right to accept or reject any or all proposals submitted pursuant to this request for proposals. Park City will provide respondents written notice of any cancellation and/or modification. Furthermore, the City shall have the right to waive any informality or technicality in proposals received when in the best interests of the City.

Park City Municipal Corporation reserves the right to reject any and all proposals for any reason. Proposals lacking required information will not be considered. All submittals shall be public records in accordance with government records regulations ("GRAMA") unless otherwise designated by the applicant pursuant to UCA §63G-2-309, as amended. The award of contract is subject to approval by City Council. If bidder utilizes third parties for completing RFP requirements, list what portion of the RFP will be completed by third parties and the name, if known, of the third party.

Price may not be the sole deciding factor.

IV. Selection Process

PCMC will evaluate proposals based on completeness, qualifications, and experience and ability to comply with requirements mentioned herein. Park City may request additional information on the proposal if insufficient or unclear details are provided. Proposals should either agree to the standard contract "as is" or request changes to the form as part of the proposal; however, RFP responders should understand that the City is not required to make adjustments to the standard contract. The nature and extent of any requested changes to the standard City contract will be considered as part of the evaluation process. The nature and extent of requested changes to our standard contract or technical requirements listed in Exhibit C to the draft contract (i.e., unwillingness to comply with our insurance/indemnity provision or technical requirements counts against a bidder). All proposals shall be good for up to one hundred eighty (180) days after receipt.

Proposals will be evaluated on the criteria listed below.

The selection process will happen in two parts. All submittals will be first evaluated on the following criteria:

1. Overall price including reoccurring maintenance over five (5) years.
2. Completeness of solution in providing: Payroll, Human Resources, Employee self-service, Timekeeping, Recruiting and Onboarding. Note that Timekeeping could be a proposed solution that integrates with Kronos 6.1 or newer.
3. Ability to implement solution: project facilitation, management and support with expected role clarity of all parties.
4. Timeline for project completion (not to exceed one year from contract award).
5. Ability to download information into current financial software Eden for payroll reconciliation with City general ledger accounts.

Once vendors have been selected from these criteria, the City will further evaluate for selection. Evaluation will continue with the information required in Attachment B. Also, the City will schedule demos with those vendors to investigate software functions and options, as well evaluate them for other functionalities. A final selection will be made at that time based on all of the above factors. Attachment B is in Excel format, and must be filled out and submitted in the same format.

The selection committee will be comprised of PCMC employees who will review the proposals based on the information provided. Following a review of the written proposals, the selection committee will make a final selection and award the services contract subject to final approval by City Council. The City reserves the right to enter into discussions with the offeror(s) determined to be reasonably susceptible of being selected for award, or to enter into exclusive discussions with the offeror whose proposal is deemed most advantageous, whichever is in the City's best interest, for the purpose of negotiation. In the event that exclusive negotiations are conducted and an agreement is not reached, the City reserves the right to enter into negotiations

with the next highest ranked offer without the need to repeat the formal solicitation process. The City reserves the right to reject any or all proposals received for any reason. Proposals lacking required information will not be considered. Furthermore, the City shall have the right to waive any informality or technical defect in proposals received when in the best interest of the City.

The selection process will proceed on the following schedule:

A. Proposals will be received by Park City prior to 5:00 pm on Thursday, October 12, 2017, to the following email address (If 8MB or less): bmoss@parkcity.org, on a Flash drive, or via Dropbox as a read-only shared link.

B. A selection committee comprised of the HR Manager, Finance Manager, and Payroll Coordinator and/or City staff will meet to review all submitted RFPs on or before Monday, October 16, 2017 5:00 p.m. MST. Initial proposals will be evaluated for price and content. Finalists will be chosen and asked to fill out the questionnaire in Attachment B and schedule a product demo within two (2) weeks. Vendors will have ten (10) working days to fill out additional information requests.

C. The selection committee may conduct additional research such as site visits to existing customers using the product (at the City's expense), customer interviews (at the City's expense), and request 30-day "proof of concept" product evaluations before selecting a finalist.

D. It is anticipated that City Council will vote on the contract award by Friday, January 5, 2018.

Park City Municipal Corporation reserves the right to change any dates or deadlines related to the bid submittal process.

V. Park City Municipal Standard Service Provider Agreement

The successful proposal will be required to enter into Park City's Professional Service Agreement, in its current form, with the City. A draft of the Agreement is attached to this RFP as Attachment A. The contract includes Exhibit "C" which lists technical and security requirements. If there is a conflict between the written and numerical amount of the proposal, the written amount shall supersede.

Any service provider who contracts with Park City is required to have a valid Park City business license, found here: http://www.parkcity.org/how-do-i/business-licenses/general-business-license.

VI. Information to be submitted

To be considered, one electronic copy of the proposal must be received by email (if 8MB or less), bmoss@parkcity.org, on a flashdrive, or via Dropbox as a read-only shared link no later than Thursday, October 21, 2017 at 5:00 p.m. MST.

VII. Preparation of Proposals

A. Failure to Read. Failure to Read the Request for Proposal and these instructions will be at the offeror's own risk.

B. Cost of Developing Proposals. All costs related to the preparation of the proposals and any related activities are the sole responsibility of the offeror. The City assumes no liability for any costs incurred by offerors throughout the entire selection process.

VIII. Proposal Information

A. Equal Opportunity. The City will make every effort to ensure that all offerors are treated fairly and equally throughout the entire advertisement, review and selection process. The procedures established herein are designed to give all parties reasonable access to the same basic information.

B. Proposal Ownership. All proposals, including attachments, supplementary materials, addenda, etc., shall become the property of the City and will not be returned to the offeror.

C. Rejection of Proposals. The City reserves the right to reject any or all proposals received. Furthermore, the City shall have the right to waive any informality or technicality in proposals received when in the best interest of the City.

D. No proposal shall be accepted from, or contract awarded to, any person, firm or corporation that is in arrears to the City, upon debt or contract, or that is a defaulter, as surety or otherwise, upon any obligation to the City, or that may be deemed irresponsible or unreliable by the City. Offerors may be required to submit satisfactory evidence that they have the necessary financial resources to perform and complete the work outlined in this RFP.

E. Park City Municipal Corporation’s policy is, subject to Federal, State and local procurement laws, to make reasonable attempts to support Park City businesses by purchasing goods and services through local vendors and service providers.

F. If bidder utilizes third parties for completing RFP requirements, list what portion of the RFP will be completed by third parties and the name, if known, of the third party.

ATTACHMENT A

PARK CITY MUNICIPAL CORPORATION
SERVICE PROVIDER/PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made and entered into in duplicate this ____ day of _____, 20__, by and between PARK CITY MUNICIPAL CORPORATION, a Utah municipal corporation, ("City"), and _____, a _____, ("Service Provider"), collectively, the City and the Service Provider are referred to as (the "Parties)."

WITNESSETH:

WHEREAS, the City desires to have certain services and tasks performed as set forth below requiring specialized skills and other supportive capabilities;

WHEREAS, sufficient City resources are not available to provide such services; and

WHEREAS, the Service Provider represents that the Service Provider is qualified and possesses sufficient skills and the necessary capabilities, including technical and professional expertise, where required, to perform the services and/or tasks set forth in this Agreement.

NOW, THEREFORE, in consideration of the terms, conditions, covenants, and performance contained herein, the Parties hereto agree as follows:

1. <u>SCOPE OF SERVICES</u>.

The Service Provider shall perform such services and accomplish such tasks, including the furnishing of all materials and equipment necessary for full performance thereof, as are identified and designated as Service Provider responsibilities throughout this Agreement and as set forth in the "Scope of Services" attached hereto as "Exhibit A" and incorporated herein (the "Project"). The total fee for the Project shall not exceed _____ Dollars ($_____).

The City has designated Brooke Moss, or his/her designee as City's Representative, who shall have authority to act in the City's behalf with respect to this Agreement consistent with the budget contract policy.

Technical requirements called out in the RFP Exhibit C must be met on an ongoing basis.

2. TERM.

No work shall occur prior to the issuance of a Notice to Proceed which cannot occur until execution of this Agreement, which execution date shall be commencement of the term and the term shall terminate on _____ or earlier, unless extended by mutual written agreement of the Parties.

3. COMPENSATION AND METHOD OF PAYMENT.

A. Payments for services provided hereunder shall be made monthly following the performance of such services.

B. No payment shall be made for any service rendered by the Service Provider except for services identified and set forth in this Agreement.

C. For all "extra" work the City requires, the City shall pay the Service Provider for work performed under this Agreement according to the schedule attached hereto as "Exhibit B," or if none is attached, as subsequently agreed to by both Parties in writing.

D. The Service Provider shall submit to the City Manager or her designee on forms approved by the City Manager, an invoice for services rendered during the pay period. The City shall make payment to the Service Provider within thirty (30) days thereafter. Requests for more rapid payment will be considered if a discount is offered for early payment. Interest shall accrue at a rate of six percent (6%) per annum for services remaining unpaid for sixty (60) days or more.

E. The Service Provider reserves the right to suspend or terminate work and this Agreement if any unpaid account exceeds sixty (60) days.

F. Service Provider acknowledges that the continuation of this Agreement after the end of the City's fiscal year is specifically subject to the City Council's approval of the annual budget.

4. RECORDS AND INSPECTIONS.

A. The Service Provider shall maintain books, records, documents, statements, reports, data, information, and other material with respect to matters covered, directly or indirectly, by this Agreement, including (but not limited to) that which is necessary to sufficiently and properly reflect all direct and indirect costs related to the performance of this Agreement, and shall maintain such accounting procedures and practices as may be necessary to assure proper accounting of all funds paid pursuant to this Agreement.

B. The Service Provider shall retain all such books, records, documents, statements, reports, data, information, and other material with respect to matters covered, directly or indirectly, by this Agreement for six (6) years after expiration of the Agreement.

C. The Service Provider shall, at such times and in such form as the City may require, make available for examination by the City, its authorized representatives, the State Auditor, or other governmental officials authorized by law to monitor this Agreement all such books, records, documents, statements, reports, data, information, and other material with respect to matters covered, directly or indirectly, by this Agreement. The Service Provider shall permit the City or its designated authorized representative to audit and inspect other data relating to all matters covered by this Agreement. The City may, at its discretion, conduct an audit at its expense, using its own or outside auditors, of the Service Provider's activities, which relate directly or indirectly to this Agreement.

D. The City is subject to the requirements of the Government Records Access and Management Act, Chapter 2, Title 63G, Utah Code Annotated, 1953, as amended and Park City Municipal Code Title 5 ("GRAMA"). All materials submitted by Service Provider pursuant to this Agreement are subject to disclosure unless such materials are exempt from disclosure pursuant to GRAMA. The burden of claiming and exemption form disclosure rests solely with Service Provider. Any materials for which Service Provider claims a privilege from disclosure based on business confidentiality shall be submitted marked as "confidential - business confidentiality" and accompanied by a concise statement from Service Provider of reasons supporting its claim of business confidentiality. Generally, GRAMA only protects against the disclosure of trade secrets or commercial information that could reasonably be expected to result in unfair competitive injury. The City will make reasonable efforts to notify Service Provider of any requests made for disclosure of documents submitted under a claim of confidentiality. Service Provider specifically waives any claims against the City related to any disclosure of materials pursuant to GRAMA.

5. <u>INDEPENDENT CONTRACTOR RELATIONSHIP</u>.

A. The Parties intend that an independent Service Provider/City relationship will be created by this Agreement. No agent, employee, or representative of the Service Provider shall be deemed to be an employee, agent, or representative of the City for any purpose, and the employees of the Service Provider are not entitled to any of the benefits the City provides for its employees. The Service Provider will be solely and entirely

responsible for its acts and for the acts of its agents, employees, subcontractors or representatives during the performance of this Agreement.

B. In the performance of the services herein contemplated the Service Provider is an independent contractor with the authority to control and direct the performance of the details of the work, however, the results of the work contemplated herein must meet the approval of the City and shall be subject to the City's general rights of inspection and review to secure the satisfactory completion thereof.

6. SERVICE PROVIDER EMPLOYEE/AGENTS.

The City may at its sole discretion require the Service Provider to remove an employee(s), agent(s), or representative(s) from employment on this Project. The Service Provider may, however, employ that (those) individuals(s) on other non-City related projects.

7. HOLD HARMLESS INDEMNIFICATION.

A. The Service Provider shall indemnify and hold the City and its agents, employees, and officers, harmless from and shall process and defend at its own expense any and all claims, demands, suits, at law or equity, actions, penalties, losses, damages, or costs, of whatsoever kind or nature, brought against the City arising out of, in connection with, or incident to the execution of this Agreement and/or the Service Provider's defective performance or failure to perform any aspect of this Agreement; provided, however, that if such claims are caused by or result from the concurrent negligence of the City, its agents, employees, and officers, this indemnity provision shall be valid and enforceable only to the extent of the negligence of the Service Provider; and provided further, that nothing herein shall require the Service Provider to hold harmless or defend the City, its agents, employees and/or officers from any claims arising from the sole negligence of the City, its agents, employees, and/or officers. The Service Provider expressly agrees that the indemnification provided herein constitutes the Service Provider's limited waiver of immunity as an employer under Utah Code Section 34A-2-105; provided, however, this waiver shall apply only to the extent an employee of Service Provider claims or recovers compensation from the City for a loss or injury that Service Provider would be obligated to indemnify the City for under this Agreement. This limited waiver has been mutually negotiated by the Parties, and is expressly made effective only for the purposes of this Agreement. The provisions of this section shall survive the expiration or termination of this Agreement.

B. Service Provider does hereby remise, release, forever discharge and covenant not to sue PARK CITY MUNICIPAL CORPORATION, its agents, servants, employees, officers, successors and assigns, and/or heirs, executors and administrators, and also any and all other persons, associations and corporations, whether herein named or referred to or not, and who, together with the above named, may be jointly and severally liable to the Service Provider, of and from any and all, and all manner of, actions and causes of action, rights, suits, covenants, contracts, agreements, judgments, claims and demands whatsoever in law or equity, including claims for contribution, arising from and by reason of any and all KNOWN AND UNKNOWN, FORESEEN AND UNFORESEEN bodily and personal injuries or death, damage to property, and the consequences thereof, which heretofore have been, and which hereafter may be sustained by the Service Provider or by any and all other persons, associations and corporations, whether herein named or referred to or not, from all liability arising out of, in connection with, or incident to the execution of this Agreement

C. No liability shall attach to the City by reason of entering into this Agreement except as expressly provided herein.

8. <u>INSURANCE</u>.

The Service Provider shall procure and maintain for the duration of the Agreement, insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the work hereunder by the Service Provider, their agents, representatives, employees, or subcontractors. The Service Provider shall provide a Certificate of Insurance evidencing:

A. General Liability insurance written on an occurrence basis with limits no less than One Million Dollars ($1,000,000) combined single limit per occurrence and Three Million Dollars ($3,000,000) aggregate for personal injury, bodily injury and property damage.

The Service Provider shall increase the limits of such insurance to at least the amount of the Limitation of Judgments described in Section 63G-7-604 of the Governmental Immunity Act of Utah, as calculated by the state risk manager every two years and stated in Utah Admin. Code R37-4-3.

B. Automobile Liability insurance with limits no less than Two Million Dollars ($2,000,000) combined single limit per accident for bodily injury and property damage.

C. Professional Liability (Errors and Omissions) insurance with annual limits no less than One Million Dollars ($1,000,000) per occurrence. If written on a claims-made basis, the Service Provider warrants that the retroactive date applicable to coverage precedes the effective date of this agreement; and that continuous coverage will be maintained for an extended reporting period and tail coverage will be purchased for a period of at least three (3) years beginning from the time that work under this agreement is complete.

D. Workers Compensation insurance limits written as follows:
Bodily Injury by Accident Five Hundred Thousand Dollars ($500,000) each accident; Bodily Injury by Disease Five Hundred Thousand Dollars ($500,000) each employee, Five Hundred Thousand Dollar ($500,000) policy limit.

E. Data Breach and Privacy / Cyber Liability Insurance including coverage for failure to protect confidential information and failure of the security of the Service Provider's computer systems or the City's systems due to the actions of the Service Provider which results in unauthorized access to the City's data. The limit applicable to this policy shall be no less than $5,000,000 per occurrence, and must apply to incidents related to the Cyber Theft of the City's property, including but not limited to money and securities.

F. Technology Errors and Omissions Insurance with a limit of not less $5,000,000 for damages arising from computer related services including but not limited to the following:

- Consulting;
- Data Processing;
- Programming;
- System Integration;
- Hardware or Software Development;
- Installation;
- Distribution or Maintenance;
- Systems Analysis Or Design;
- Training; and
- Staffing or Other Support Services.

The policy shall include coverage for third party fidelity including cyber theft and protect the City as "Additional Insured". It is acceptable that the Data Breach and Privacy / Cyber Liability Insurance and Technology Errors and Omissions insurance be provided on the same policy. The

total cost of the insurance, as listed above, must be incorporated into the Cost Proposal. The additional insured protection afforded the City must be on a primary and non-contributory basis. All policies must include a waiver of subrogation in favor of the City.

G. The City shall also be named as an additional insured on general liability and auto liability insurance policies, with respect to work performed by or on behalf of the Service Provider and a copy of the endorsement naming the City as an additional insured shall be attached to the Certificate of Insurance. Should any of the above described policies be cancelled before the expiration date thereof, Service Provider shall deliver notice to the City within thirty (30) days of cancellation. The City reserves the right to request certified copies of any required policies.

H. The Service Provider's insurance shall contain a clause stating that coverage shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.

9. TREATMENT OF ASSETS.

Title to all property furnished by the City shall remain in the name of the City and the City shall become the owner of the work product and other documents, if any, prepared by the Service Provider pursuant to this Agreement (contingent on City's performance hereunder).

10. COMPLIANCE WITH LAWS AND WARRANTIES.

A. The Service Provider, in the performance of this Agreement, shall comply with all applicable federal, state, and local laws and ordinances, including regulations for licensing, certification and operation of facilities, programs and accreditation, and licensing of individuals, and any other standards or criteria as described in this Agreement to assure quality of services.

B. Unless otherwise exempt, the Service Provider is required to have a valid Park City business license.

C. The Service Provider specifically agrees to pay any applicable fees or charges which may be due on account of this Agreement.

D. If this Agreement is entered into for the physical performance of services within Utah the Service Provider shall register and participate in E-Verify, or equivalent program. The Service Provider agrees to verify employment eligibility through E-Verify, or equivalent program, for each new employee

that is employed within Utah, unless exempted by Utah Code Ann. § 63G-12-302.

E. Service Provider shall be solely responsible to the City for the quality of all services performed by its employees or sub-contractors under this Agreement. Service Provider hereby warrants that the services performed by its employees or sub-contractors will be performed substantially in conformance with the standard of care observed by similarly situated companies providing services under similar conditions.

11. NONDISCRIMINATION.

A. The City is an equal opportunity employer.

B. In the performance of this Agreement, the Service Provider will not discriminate against any employee or applicant for employment on the grounds of race, creed, color, national origin, sex, marital status, age or the presence of any sensory, mental or physical handicap; provided that the prohibition against discrimination in employment because of handicap shall not apply if the particular disability prevents the proper performance of the particular worker involved. The Service Provider shall ensure that applicants are employed, and that employees are treated during employment without discrimination because of their race, creed, color, national origin, sex, marital status, age or the presence of any sensory, mental or physical handicap. Such action shall include, but not be limited to: employment, upgrading, demotion or transfers, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and programs for training including apprenticeships. The Service Provider shall take such action with respect to this Agreement as may be required to ensure full compliance with local, state and federal laws prohibiting discrimination in employment.

C. The Service Provider will not discriminate against any recipient of any services or benefits provided for in this Agreement on the grounds of race, creed, color, national origin, sex, marital status, age or the presence of any sensory, mental or physical handicap.

D. If any assignment or subcontracting has been authorized by the City, said assignment or subcontract shall include appropriate safeguards against discrimination. The Service Provider shall take such action as may be required to ensure full compliance with the provisions in the immediately preceding paragraphs herein.

12. ASSIGNMENTS/SUBCONTRACTING.

A. The Service Provider shall not assign its performance under this Agreement or any portion of this Agreement without the written consent of the City, and it is further agreed that said consent must be sought in writing by the Service Provider not less than thirty (30) days prior to the date of any proposed assignment. The City reserves the right to reject without cause any such assignment. Any assignment made without the prior express consent of the City, as required by this part, shall be deemed null and void.

B. Any work or services assigned hereunder shall be subject to each provision of this Agreement and property bidding procedures where applicable as set forth in local, state or federal statutes, ordinance and guidelines.

C. Any technical/professional service subcontract not listed in this Agreement, must have express advance approval by the City.

D. Each subcontractor that physically performs services within Utah shall submit an affidavit to the Service Provider stating that the subcontractor has used E-Verify, or equivalent program, to verify the employment status of each new employee, unless exempted by Utah Code Ann. § 63G-12-302.

13. CHANGES.

Either party may request changes to the scope of services and performance to be provided hereunder, however, no change or addition to this Agreement shall be valid or binding upon either party unless such change or addition be in writing and signed by both Parties. Such amendments shall be attached to and made part of this Agreement.

14. PROHIBITED INTEREST, NO THIRD PARTY RIGHTS AND NO GRATUITY TO CITY EMPLOYEES.

A. No member, officer, or employee of the City shall have any interest, direct or indirect, in this Agreement or the proceeds thereof.

B. Nothing herein is intended to confer rights of any kind in any third party.

C. No City employee who has procurement decision making authority and is engaged in the procurement process, or the process of administering a contract may knowingly receive anything of value including but not limited

to gifts, meals, lodging or travel from anyone that is seeking or has a contract with the City.

15. MODIFICATIONS TO TASKS AND MISCELLANEOUS PROVISIONS.

A. All work proposed by the Service Provider is based on current government ordinances and fees in effect as of the date of this Agreement.

B. Any changes to current government ordinances and fees which affect the scope or cost of the services proposed may be billed as an "extra" pursuant to Paragraph 3(C), or deleted from the scope, at the option of the City.

C. The City shall make provision for access to the property and/or project and adjacent properties, if necessary for performing the services herein.

16. TERMINATION.

A. Either party may terminate this Agreement, in whole or in part, at any time, by at least thirty (30) days' written notice to the other party. The Service Provider shall be paid its costs, including contract close-out costs, and profit on work performed up to the time of termination. The Service Provider shall promptly submit a termination claim to the City. If the Service Provider has any property in its possession belonging to the City, the Service Provider will account for the same, and dispose of it in a manner directed by the City.

B. If the Service Provider fails to perform in the manner called for in this Agreement, or if the Service Provider fails to comply with any other provisions of the Agreement and fails to correct such noncompliance within three (3) days' written notice thereof, the City may immediately terminate this Agreement for cause. Termination shall be effected by serving a notice of termination on the Service Provider setting forth the manner in which the Service Provider is in default. The Service Provider will only be paid for services performed in accordance with the manner of performance set forth in this Agreement.

17. NOTICE.

Notice provided for in this Agreement shall be sent by certified mail to the addresses designated for the Parties on the last page of this Agreement. Notice is effective upon the date it was sent, except that a notice of termination pursuant

to paragraph 16 is effective upon receipt. All reference to "days" in this Agreement shall mean calendar days.

18. ATTORNEYS FEES AND COSTS.

If any legal proceeding is brought for the enforcement of this Agreement, or because of a dispute, breach, default, or misrepresentation in connection with any of the provisions of this Agreement, the prevailing party shall be entitled to recover from the other party, in addition to any other relief to which such party may be entitled, reasonable attorney's fees and other costs incurred in connection with that action or proceeding.

19. JURISDICTION AND VENUE.

A. This Agreement has been and shall be construed as having been made and delivered within the State of Utah, and it is agreed by each party hereto that this Agreement shall be governed by laws of the State of Utah, both as to interpretation and performance.

B. Any action of law, suit in equity, or judicial proceeding for the enforcement of this Agreement, or any provisions thereof, shall be instituted and maintained only in any of the courts of competent jurisdiction in Summit County, Utah.

20. SEVERABILITY AND NON-WAIVER.

A. If, for any reason, any part, term, or provision of this Agreement is held by a court of the United States to be illegal, void or unenforceable, the validity of the remaining provisions shall not be affected, and the rights and obligations of the Parties shall be construed and enforced as if the Agreement did not contain the particular provision held to be invalid.

B. If it should appear that any provision hereof is in conflict with any statutory provision of the State of Utah, said provision which may conflict therewith shall be deemed inoperative and null and void insofar as it may be in conflict therewith, and shall be deemed modified to conform in such statutory provisions.

C. It is agreed by the Parties that the forgiveness of the non-performance of any provision of this Agreement does not constitute a subsequent waiver of the provisions of this Agreement. No waiver shall be effective unless it is in writing and signed by an authorized representative of the waiving party.

21. ENTIRE AGREEMENT.

The Parties agree that this Agreement is the complete expression of the terms hereto and any oral representations or understandings not incorporated herein are excluded. Further, any modification of this Agreement shall be in writing and signed by both Parties. Failure to comply with any of the provisions stated herein shall constitute material breach of contract and cause for termination. Both Parties recognize time is of the essence in the performance of the provisions of this Agreement.

IN WITNESS WHEREOF the Parties hereto have caused this Agreement to be executed the day and year first hereinabove written.

PARK CITY MUNICIPAL CORPORATION
445 Marsac Avenue

Post Office Box 1480
Park City, UT 84060-1480

_____
Diane Foster, City Manager

Attest:

_____
City Recorder's Office

Approved as to form:

_____
City Attorney's Office

SERVICE PROVIDER NAME
Address:
Address:
City, State, Zip:

Tax ID#:
_____
PC Business License#
BL_____

_____
Signature

_____
Printed name

_____
Title

STATE OF UTAH)
) ss.
COUNTY OF SUMMIT)

On this ____ day of _____, 20__, personally appeared before me _____, whose identity is personally known to me/or proved to me on the basis of satisfactory evidence and who by me duly sworn/affirmed, did say that he/she is the _____ (title or office) of _____, a _____ corporation (or limited liability company), by Authority of its Bylaws/Resolution of the Board of Directors or Member Resolution, and acknowledged that he/she signed it voluntarily for its stated purpose as _____ (title) for _____, a _____ corporation (or limited liability company).

_____
Notary Public

EXHIBIT "A"

SCOPE OF SERVICES

EXHIBIT "B"

PAYMENT SCHEDULE FOR "EXTRA" WORK

EXHIBIT "C"
Technology Support, Infrastructure & Security

1.0 Definitions

"City Data" is any data provided, shared, created, or managed by the City.

"Service Provider" Is the contract holder that manages employees, contractors, or affiliates having access to PCMC infrastructure or data for specific defined purposes.

"Confidentiality Agreement" is defined as a legal agreement between Service Provider and one or more parties that is used to signify a confidential relationship exists between the parties. A confidentiality agreement is used in processes where various parties become privy to sensitive data/information, which is protected from access or general distribution.

"Personally Identifiable Information (PII)" is defined by NIST Special Publication 800-122. PII is any City Data relating to an identified or identifiable individual (such as name, postal address, email address, telephone number, date of birth, social security number (or its equivalent),driver's license number, account number, personal identification number, health or medical information, or any other unique identifier, or one or more factors specific to the individual's physical, physiological, mental, economic, human resource, or social identity/rating), whether such data is in individual or aggregate form and regardless of the media in which it is contained, that may be (i) disclosed at any time to Service Provider in anticipation of, in connection with, or incidental to the performance of services for or on behalf of City; (ii) Processed (as defined below) at any time by Service Provider in connection with or incidental to the performance of this Document; or (iii) derived by Service Provider from the information described in (i) and (ii) above.

"Process, Processed, or Processing" means any operation or set of operations performed upon City Data, whether or not by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, or destroying the data.

"Data Masking" The process of modifying records to conceal City Data, especially when such records are copied from a production environment to a non-production environment.

"Information Processing System(s)" is defined as the individual and collective electronic, mechanical, or software components of Service Provider operations that store and/or process City Data

“Information Security Event” is defined as any situation where PII is lost; is subject to unauthorized or inappropriate access, use, or misuse; the security, confidentiality, or integrity of the information is compromised; or the availability of Service Provider Information Processing Systems is compromised by external attack.

“Information Technology Department” is the City department responsible technology matters for the City. The Information Technology Department can be reached at 435-615-5123, or via email to: 5123@parkcity.org.

“Service Provider’s Third Party Security Auditor” is defined as a third party organization which provides security audits of Service Provider’s Information Processing Systems.

“Service Provider Confidentiality Agreement” is defined as a non-disclosure agreement executed between Service Provider and City as a prerequisite for obtaining a copy of the Service Provider Third Party Auditor’s Security Report.

“Provider” is defined as any company supplying a service for Service Provider’s Information Processing System (such as a Data Center, Managed Service, or Data Circuit).

“Security Breach” is defined as an unauthorized access to Service Provider’s software or Data Center facilities, Information Processing Systems, or networks used to service, store, or access City Data.

“Sensitive Information” is defined as any Personally Identifiable Information or any information not publicly available (i.e. – clients, financial information, employee information, schedules, technology infrastructure, etc.).

“Written Request of the City” is defined as a request received by Service Provider by a City on official letterhead signed by an officer of the City.

2.0 Protection and retention of forms and documentation

A. It is the policy of Service Provider that PII, as defined herein, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form must

be retained for at least six (6) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within Service Provider.

3.0 Security and Confidentiality

Before receiving, or continuing to receive, PII, Service Provider will implement and maintain an information security program that ensures: 1) PII and Service Provider's Information Processing Systems are protected from internal and external security threats; and 2) that PII is protected from unauthorized disclosure.

All Information Processing Systems involving City Data shall be completed within the United States or the country in which the PII was originally delivered. Any Processing performed offshore shall not include any Sensitive Information.

4.0 Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification, the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format. The following levels are to be used when classifying information:

4.1 Personally Identifiable Information

a) PII (NIST Special Publication 800-122) is any City Data relating to:

an identified or identifiable individual (such as name, postal address, email address, telephone number, date of birth, Social Security number (or its equivalent), driver's license number, account number, personal identification number, health or medical information, or any other unique identifier, or one or more factors specific to the individual's physical, physiological, mental, economic, human resource, or social identity/rating), whether such data is in individual or aggregate form and regardless of the media in which it is contained, that may be
(i) disclosed at any time to Service Provider in anticipation of, in connection with, or incidental to the performance of services for or on behalf of City;

(ii) Processed (as defined below) at any time by Service Provider in connection with or incidental to the performance of this Document; or (iii) derived by Service Provider from the information described in (i) and (ii) above.

b) Unauthorized or improper disclosure, modification, or destruction of this information could violate State and federal laws, result in civil and criminal penalties, and cause serious damage to Service Provider.

4.2 Internal Information

a) Internal Information is intended for unrestricted use within PCMC, and in some cases within affiliated organizations such as Service Provider business partners. This type of information is already widely-distributed within PCMC, or it could be so distributed within the organization without advance permission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, and most internal electronic mail messages.

b) Any information not explicitly classified as Sensitive Information, PII or Public will, by default, be classified as Internal Information.

c) Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

4.3 Public Information

a) Public Information has been specifically approved for public release by a designated authority within each entity of Service Provider. Examples of Public Information may include material posted to approved public internet web pages.

b) This information may be disclosed outside of Service Provider.

5.0 Security Policy

5.1 Formal Security Policy. Consistent with the requirement of this Document, Service Provider will create and provide to City an information security policy that is approved by Service Provider's management, published and communicated and agreed to be adhered to by all Service Provider's employees, contractors, and affiliates.

5.2 Security Policy Review. Service Provider will review the information security policy at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness and may revise such policy, from time to time. Changes resulting in a lower

standard of security or service must be agreed to by PCMC prior to adoption.

6.0 Asset Management.

6.1 Asset Inventory. Service Provider will maintain an inventory of all Service Provider Information Processing Systems and media containing Sensitive Information.

6.2 Acceptable Use. Service Provider will implement policies and procedures for the acceptable use of information and assets which is no less restrictive than industry best practice for the classification of such Information and consistent with the requirements of this Document.

6.3 Equipment Use While on City Premises. While on City's premises, Service Provider will not connect hardware (physically or via a wireless connection) to City internal systems or networks unless necessary for Service Provider to perform Processing under this Document. This hardware is subject to be inspected and/or scanned by PCMC IT Department before use, at City's request.

6.4 Portable Devices. Sensitive Information, with the exception of Business Contact Information, may not be stored on portable devices including, but not limited to, mobile computers, Phones, MP3 devices, and USB devices.

6.5 Personally-owned Equipment. Sensitive Information, with the exception of Business Contact Information, may not be stored on any employee owned equipment.

7.0 Human Resources Security

7.1 Security Awareness Training. Prior to Service Provider employees receiving access to Sensitive Information, they will receive security awareness training appropriate to their job function. Service Provider will also ensure that recurring security awareness training is performed, at intervals determined to be suitable by Service Provider. Employees are also required to receive security training on security topics such as the safe use of the Internet, working from remote locations safely, and how to label and handle sensitive data. Additional training is routinely given on policy topics of interest, including in areas of emerging technology, such as the safe use of mobile devices and social technologies.

7.2 Removal of Access Rights. The access rights of all Service Provider employees to Service Provider Information Processing Systems or media containing Sensitive Information will be removed immediately upon

termination of their employment, contract, or agreement, or adjusted upon change.

7.3 Background Checks and Restrictions.

7.3.1 Upon hire, Service Provider will verify an individual's previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, Service Provider will also conduct criminal, credit, and security checks to the extent dependent on the desired position.

7.3.2 Upon acceptance of employment at Service Provider, all employees are required to execute a confidentiality agreement and must acknowledge receipt of and compliance with policies in Service Provider's Employee Handbook. The confidentiality and privacy of City information and data is emphasized in the handbook and during new employee orientation.

7.3.3 In no event will Service Provider use the services of an individual who has been convicted of any crime involving violence or sexual assault, or who has been found civilly liable for any act of violence or sexual harassment. Service Provider agrees to provide proof of its background check process for this provision upon the Written Request of the City.

7.3.4 In no event will Service Provider, in the performance of this Document, use the services of an employee or agent who has been convicted of a felony involving dishonesty or a breach of trust without first complying with the provisions of 18 U.S. Code Section 1033. Service Provider has the responsibility to assure the compliance of its subcontractors with this requirement.

8.0 Physical and Environmental Security.

8.1 Secure Areas. Service Provider will secure all areas, including loading docks, holding areas, telecommunications areas, cabling areas, and off-site areas that contain Information Processing Systems or media containing Sensitive Information by the use of appropriate security controls in order to ensure that only authorized personnel are allowed access, and to prevent damage and interference. The following controls will be implemented:

8.1.1 Access will be controlled and restricted by use of a defined security perimeter, appropriate security barriers, entry controls, and authentication controls. A record of all accesses will be securely maintained.

8.1.2 All personnel will be required to wear some form of visible identification to identify them as employees, contractors, visitors, etc. Personal recognition of employees if possible is also acceptable.

8.1.3 Visitors to secure areas will be supervised, or cleared for non-escorted accessed, via an appropriate background check. Their date and time of entry and departure will be recorded.

8.2 Geographic Data Centers

Service Provider's data centers are geographically distributed and employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at each Service Provider data center include the following: custom designed electronic card access control systems, alarm systems, interior and exterior cameras, and security guards. Access to areas where systems, or system components, are installed or stored are segregated from general office and public areas such as lobbies. The areas are centrally monitored for suspicious activity, and the facilities are routinely patrolled by security guards.

8.3 Environmental Security

Service Provider will protect equipment from power failures and other disruptions caused by failures in supporting utilities. To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Service Provider implements a disaster recovery program at all of its data centers. This program includes multiple components to minimize the risk of any single point of failure.

8.4 Role Based Access

Service Provider restricts access to its data centers based on role, not position. As a result, most senior executives at Service Provider do not have access to Service Provider data centers.

9.0 Communications and Operations Management.

9.1 Protections Against Malicious Code. Service Provider will implement detection, prevention, and recovery controls to protect against malicious software, which is no less than current industry best practice, and perform appropriate employee training on the prevention and detection of malicious software.

9.2 Back-ups. Service Provider will perform appropriate back-ups of Service Provider Information Processing Systems and media containing City Data every business day with end-of-month copy stored for 1-year in order to ensure services and service levels described in this Document. Service Provider maintains a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain Sensitive Information and Internal Information.

9.3 Media Handling. Service Provider will protect against unauthorized access or misuse of City Data contained on media.

9.4 Media and Information Disposal. Service Provider will securely and safely dispose of media containing Sensitive Information:

9.4.1 Dispose of media containing Sensitive Information so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing or overwriting in compliance with DoD Standard 5220.22-M.

9.4.2 Maintain a secured disposal log that provides an audit trail of disposal activities.

9.4.3 Provide a certificate of destruction to City certifying that all Sensitive Information was purged. The certificate will be provided to City upon Written Request of the City within ten (10) business days after the information was purged.

9.5 Exchange of Information

To protect confidentiality and integrity of Sensitive Information in transit, Service Provider will:

9.5.1 Perform an inventory, analysis, and risk assessment of all data exchange channels (including, but not limited to, SFTP, HTTP, HTTPS, SMTP, modem, and fax) to identify and mitigate risks to Sensitive Information from these channels.

9.5.2 Monitor and inspect all data exchange channels to detect unauthorized information releases.

9.5.3 Ensure that appropriate security controls using approved data exchange channels are employed when exchanging Sensitive Information.

9.5.4 Employ industry standard enhanced security measures (at a minimum 256-bit Triple DES encryption) to encrypt Sensitive Information.

9.5.5 Ensure any media containing Sensitive Information is encrypted in compliance with the requirements set forth above and via a carrier where a unique auditable tracking number is provided per shipment.

9.6 Monitoring

To protect against unauthorized access or misuse of Sensitive Information residing on Service Provider Information Processing Systems, Service Provider will:

9.6.1 Employ current industry best practice security controls and tools to monitor Information Processing Systems and log user activities, exceptions, unauthorized information processing activities, suspicious activities, and information security events. Logging facilities and log information will be protected against tampering and unauthorized access. Logs will be kept for at least one hundred eighty (180) days.

9.6.2 Perform frequent reviews of logs and take necessary actions to protect against unauthorized access and implement policy and infrastructure as needed.

9.6.3 At Written Request of the City, make logs available to City to assist in investigations.

9.6.4 Comply with all relevant legal regulations applicable to monitoring and logging activities.

9.6.5 Ensure that the time clocks of all relevant Information Processing Systems are synchronized using a national or international time source.

9.6.6 Ensure common configuration and patch management information is maintained.

9.6.7 Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

10.0 Access Control

10.1 User Access Management. To protect against unauthorized access or misuse of Sensitive Information, a formal user registration and de-registration procedure for granting and revoking access and access rights to all Service Provider Information Processing Systems.

10.1.2 Employ a formal password management process using authentication and authorization controls that are designed to protect against unauthorized access.

10.1.3 Perform recurring reviews of Service Provider employees' access and access rights to ensure that they are appropriate for the users' role.

10.2 User Responsibilities

To protect against unauthorized access or misuse of Sensitive Information residing on Service Provider Information Processing Systems, Service Provider will:

10.2.1 Ensure that Service Provider Information Processing Systems users follow current security practices in the selection and use of sufficiently strong passwords.

10.2.2 Ensure that unattended equipment has appropriate protection to prohibit access and use by unauthorized individuals.

10.2.3 Ensure that Sensitive Information contained at employee workstations, including, but not limited to, paper and media display screens, is protected from unauthorized access.

10.3 Network Access Control

Access to internal, external, and public network services that allow access to Service Provider Information Processing Systems shall be controlled. Service Provider will:

10.3.1 Ensure that current industry best practice standard authentication mechanisms for network users and equipment are in place and updated as necessary.

10.3.2 Ensure electronic perimeter controls are in place to protect Service Provider Information Processing Systems from unauthorized access.

10.3.3 Ensure sufficient authentication methods are used to control access by remote users.

10.3.4 Ensure physical and logical access to diagnostic and configuration ports is controlled.

10.4 Operating System Access Control

To protect against unauthorized access or misuse of Sensitive Information residing on Service Provider Information Processing Systems, Service Provider will:

10.4.1 Ensure that access to operating systems is controlled by a secure log-on procedure and limited to role based necessity.

10.4.2 Ensure that Service Provider Information Processing System users have a unique identifier (user ID). This account is used to identify each person's activity on Service Provider's Information Processing Systems network, including any access to employee or City data.

10.4.3 Ensure that the use of utility programs that are capable of overriding system and application controls are highly restricted and tightly controlled, with access limited to those employees whose specific job function requires such access.

10.4.4 Ensure that inactive sessions are automatically terminated when technically possible after a defined period of inactivity.

10.4.5 Employ idle time-based restrictions on connection times when technically possible to provide additional security for high risk applications.

10.5 Wireless Network Access Control. Wireless Access will be provided to access networks which do not store or process Sensitive Information. Service Provider will:

10.5.1 Ensure that current industry best practice standard authentication mechanisms for wireless network users and equipment are in place and updated as necessary.

10.5.2 Ensure authentication methods are used to control access by remote users, with unique User Identifiers.

11.0 Information Systems Acquisition, Development and Maintenance

11.1 Security of System Files. To protect City Information Processing Systems and system files containing Sensitive Information, Service Provider will ensure that access to source code is restricted to authorized users whose specific job function necessitates such access.

11.2 Security in Development and Support Processes. To protect City information Processing Systems and system files containing Sensitive Information, Service Provider will:

11.2.1 Ensure that the implementation of changes is controlled and documented by the use of formal change control procedures.

11.2.2 Employ industry best practice security controls to minimize information dissemination.

11.2.3 Employ oversight quality controls and security management of outsourced software development.

11.2.4 Employ regular perimeter security reviews for all external interfaces to Sensitive Information.

11.2.5 Employ regular code reviews covering security vulnerabilities, including, but not limited to, buffer overflow, SQL injection, input validation, and commonly used vector attacks.

11.3 SSAE16

11.3.1 Service Provider agrees to follow reasonable industry standards for physical security for the Information it receives under this Document, including, but not limited to:

(1) encryption of Sensitive Information while in transit or stored on Service Provider's network; (2) Logical separation of each City's Sensitive Information from other records location at Service Provider's location(s); (3) job function based restriction on a "need to know basis" for access to PII at Service Provider's location; (4) monitoring by appropriate systems to detect attacks or intrusions via internal or external sources; (5) protection against losses of the Information due to fire, water, or other environmental causes; (6) adequately developed and tested backup/recovery plans.

11.3.2 Service Provider agrees to maintain a SSAE16, Type 2 certification for all physical data centers. The SSAE16 audit shall be completed every twelve (12) months. Service Provider agrees on an ongoing basis to annually provide City a copy of its most recent SSAE16, Type 2 audit applicable to all physical access to systems and networks involved in Service Provider's performance of this Document upon Written Request of the City.

11.4 Terms for Internet Commerce

11.4.1 Service Provider agrees to follow reasonable industry standards for physical security for the Sensitive Information received, including but not limited to:

11.4.2 Encryption. All Sensitive Information transmitted over the Internet shall be encrypted using no less than 256 bit encryption, while in transit or stored on Service Provider's network.

11.4.3 Storage. Service Provider shall store all PII on a secured server behind a firewall. Service Provider shall take all reasonably necessary steps to limit access to Sensitive Information to those employees or agents of Service Provider who have a legitimate business need to access the Information.

11.4.4 Authentication Credentials. Service Provider shall limit access to its web site by providing unique user IDs and passwords to all authorized users ("Authentication Credentials"). Service Provider may not allow more than one person to use the same Authentication Credentials to access any Sensitive Information. Service Provider shall provide for separate Authentication Credentials for each City employee who may require access to its web site or system for any purpose related to this Document.

11.4.5 Password Encryption. All City passwords stored at the Service Provider's site shall be secured using no less than 256 bit encryption or another functionally equivalent safeguard that is intended to protect passwords from disclosure,

11.4.6 Security Administration. Service Provider shall provide for monitoring by appropriate systems to detect attacks or intrusions via internal or external sources; protection against losses of the Information due to fire, water or other environmental causes; and adequately developed and tested backup/recovery plans.

12.0 Information Security Incident Management

12.1 Reporting Information Security Events and Weaknesses. To protect City Information Processing Systems and system files containing Sensitive Information, Service Provider will:

12.1.1 Implement a process to ensure that Information Security Events and Security Breaches are reported through appropriate management channels as quickly as possible.

12.1.2 Train all employees, contractors, users of information systems and services regarding the report of any observed or suspected Information Security Events and Security Breaches.

12.1.3 Notify City by email or phone as soon as possible of all Information Security Events and Security Breaches. Following any such event or breach, Service Provider will promptly notify City whether or not Sensitive Information was compromised or released to unauthorized parties, the data affected, and/or the details of the event or breach.

13.0 Business Continuity Management

13.1 Business Continuity Management Program. To ensure services and service levels described in this Document, Service Provider will:

13.1.1 Develop and maintain a process for business continuity throughout the organization that addresses the information security requirements needed for Service Provider's and its Providers' business continuity so that the provision of products and/or services provided is uninterrupted.

13.1.2 Maintain efforts to identify events that may cause interruptions to business processes, along with the probability and impact of such interruptions and the consequences for information security.

13.1.3 Develop and implement plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes, and provide City a copy of the same upon Written Request of the City.

13.1.4 Test and update business continuity plans to ensure that they are up-to-date and effective.

13.2 Disaster Recovery. Service Provider has appropriate and reasonable disaster recovery measures in place designed to prevent any interruptions in Service to the City. Service Provider has established disaster contingency plans governing processes following a breach incident, which in particular address the following issues: (i) safety of personnel and third parties, (ii) losses of communications capability (e.g., voice, fax, data), (iii) loss of computer processing capabilities, and (iv) loss of access to physical office facilities.

14.0 Security Assessments

14.1 Initial and Recurring Security Assessments. Service Provider's Third-Party Security Auditor shall perform weekly static scans, monthly dynamic

scans, and annual penetration testing. The results of these audits are available to Service Provider and the City with execution of a Confidentiality Agreement with Service Provider.

15.0 Force Majeure

Neither party shall be liable for any delays in performance hereunder due to circumstances beyond its control including, but not limited to, acts of nature, acts of governments, delays in transportation, and delays in delivery or inability of Service Provider's partners or Service Providers to deliver.

16.0 Compliance

Service Provider agrees to implement and maintain measures to comply with any applicable State or federal law or regulation governing the provision, receipt, maintenance, storage, or destruction of Sensitive Information.