Request for Proposals (RFP) (NON-BID)

for

EMERGENCY AND ON-CALL WATER SYSTEM SCADA INTEGRATOR SERVICES

Park City Municipal Corporation (PCMC)

P.O. Box 1480

Park City, Utah 84060

Issued May 7, 2024

Respondents and their agents are instructed not to contact PCMC employees, agents or contractors of PCMC, selection committee members, the Mayor's office or staff, members of the City Council, or attempt to externally manipulate or influence the procurement process in any way, other than through the instructions contained herein, from the date of release of this RFP to the date of execution of the agreement resulting from this solicitation. PCMC, in its sole discretion, may disqualify a Respondent for violation of this provision.

REQUEST FOR PROPOSALS (RFP)

PCMC is inviting proposals ("Proposals") from qualified persons or firms ("Respondents") to provide **Water System SCADA Integrator Services.**

PROPOSALS DUE: **By 3:00 p.m. on Tuesday, May 28, 2024**

Submit Proposals electronically *via email to jason.christensen@parkcity.org*. The Proposals will be opened after the submission deadline.

In the event of difficulty submitting Proposals electronically, Proposals can be dropped off at the office of the City Recorder, located at 445 Marsac Avenue, Third Floor – Executive Department, Park City, UT 84060. Proposals submitted to the City Recorder should be delivered on a zip drive. No paper copies should be submitted.

RFP AVAILABLE: The RFP will be available on May 7, 2024, on the Utah Public Procurement Place (U3P) and PCMC websites. Any modifications to the RFP or responses to questions submitted will be added as an addendum to the RFP posted on the U3P and PCMC websites. It is the responsibility of Respondents to regularly check for addenda.

QUESTIONS: All questions regarding the RFP must be submitted in writing by email to jason.christensen@parkcity.org by **4:00 p.m. on Tuesday, May 21, 2024.** Please do not submit the same question multiple times.

PROJECT DESCRIPTION (brief): Provide water system supervisory control and data acquisition (SCADA) integrator services for our existing SCADA water system. More specifically, on-call and emergency services involving updates, modifications, troubleshooting, programing, integration, software and hardware acquisition, installation, testing and start-up.

OWNER:	Park City Municipal Corporation P.O. Box 1480 Park City, UT 84060
CONTACT:	*Jason Christensen, Water Resources Manager* *jason.christensen@parkcity.org*

Proposals will remain valid for 90 days after submission. PCMC reserves the right to reject any or all Proposals received for any reason. Furthermore, PCMC reserves the right to change dates or deadlines related to this RFP. PCMC also reserves the right to waive any informality or technicality in Proposals received when in the best interest of PCMC.

1.0 INTRODUCTION

PCMC, located in Summit County, Utah, is soliciting written Proposals from qualified firms ("Respondents") to provide water system SCADA Integrator services.

This is a solicitation for on-call and emergency 24-hour services related to updates, modifications, troubleshooting, programming, integration, software and hardware acquisition, installation, testing, and start-up.

PCMC intends to select one or more Respondents to provide services as outlined in this RFP that meet the City's overall system needs, goals, and objectives.

1.1 PCMC Public Utilities

PCMC Public Utilities provides culinary water to approximately 5,600 residential and business connections within Park City via a water treatment, supply, and distribution system. PCMC maintains over 140 miles of pipeline, 5,600 meters, 5,000-meter pits, and 5,000 service lines. In addition, PCMC maintains three state-of-the-art water treatment facilities and three wells.

Additional information about PCMC can be found on its website at: www.parkcity.org.

The PCMC SCADA system generally consists of the following:

- Approximately 70 remote sites in total. Roughly 45 sites are equipped with Allen Bradley CompactLogix PLCs; 39 of the 45 sites communicate using Cisco Fluidmesh (FM) radios and the remaining 6 have been connected to a City-owned fiber optic network for communications with the central SCADA server. Approximately 25 monitoring-only sites utilize either Phoenix Contact wireless IO radios, or FreeWave ZumLink radios where the signal is sent to a nearby remote site outfitted with a Programmable Logic Controller (PLC).
- Three water treatment plants outfitted with Allen Bradley ControlLogix PLCs. These plants are connected to a City-owned fiber optic network for communications with the central SCADA server. The treatment plans have a fallback SCADA server that takes control in the event of connectivity issues.
- The central SCADA site includes two redundant virtual servers running Inductive Automation's Ignition platform and a SQL cluster database that acts as a centralized historian server. The central SCADA site is connected to the City-owned fiber-optic network.
- Operators remotely access the Ignition HMI using laptops after connecting to the City network over a VPN.

2.0 Scope Of Services

PCMC is soliciting Water System SCADA Integrator Services for On-Call and Emergency assistance to PCMC for services related to updates, modifications, troubleshooting, programming,

integration, software and hardware acquisition, installation, testing, and start-up. One or more Respondents may be selected.

Services requested may include on-site maintenance at any office or location of PCMC; although to the extent reasonable and customary under the circumstances, services may be provided remotely.

PCMC will notify the on-call service provider of the needed action and issue a work order for the work. PCMC reserves the right to contract with multiple vendors and reserves the right to select any vendor for a work order project. Subject to negotiations with one or more successful Respondents, a five-year term is being proposed during which successful Respondents will be able to provide services to PCMC.

The following is a non-exclusive list of work that may be requested:

1. Corrective Maintenance
2. Preventative Maintenance
3. SCADA System Software Updating and Testing
4. Corrective and Preventative Maintenance of Allen Bradley Programmable Logic Controllers (PLCs)
5. Documentation & Revision Control

General Service Terms and Conditions

Response Times. "Regular Response" requires a response within 7 days of notification by PCMC, and continuous work during regular business hours until resolved. "Emergency Response" requires a response within 2 hours of notification, and continuous work until the problem is resolved, or a workaround is implemented.

Hours of Service. Support shall be available 24 hours a day, seven days a week, including holidays. Normal business hours are from 7:00 am to 5:00 pm Monday – Friday, excluding PCMC holidays.

Telephone and Email Support. Provide a designated contact for telephone and email support that will be available both during and after business hours to respond to issues.

Records and Reports. Maintain records and statistics of any maintenance provided, including:

a. Date, time and name of contact.
b. Equipment being serviced.
c. All steps and actions taken to maintain the equipment or repair the problem.
d. All equipment and/or labor costs associated with the maintenance or problem.

3.0 PROPOSAL REQUIREMENTS AND CONTENTS

3.1 General

Proposals should include the following key elements per the instructions and requirements set out in this RFP.

3.2 Proposal Format

Proposals should be as concise as possible while adhering to the format and information requirements described below. Any page limits identified do not include table of contents, dividers, etc.

Respondents shall provide sufficient information in Proposals to enable PCMC to understand and evaluate the Respondent's approach to providing the services described in this RFP. At a minimum, each Proposal shall respond to the following requirements which are listed below and further described in the following paragraphs:

Organize Proposals as Follows. Proposals not organized as outlined below, not containing the information specified, or not containing sufficient detail may receive a lower rating when evaluated.

PART 1 – Proposer Identification and Organization

Section A. Letter of Introduction

Section B. Client References

Section C. Insurance Professional Services Agreement – Cyber Standard Requirements

PART 2 - Technical Response

Section A. Organization and Key Personnel

Section B. Summary

PART 3 - Attachments

Exhibit A. Professional Services Agreement – Cyber Standard

PART 1 – Proposer Identification and Organization

A. LETTER OF INTRODUCTION

Two Page Limit.

Please provide a letter of introduction that briefly:

1. States Respondent’s interest in providing SCADA Integrator Services to PCMC.
2. Acknowledges receipt of RFP addenda, if any.
3. Identifies the name of the Respondent firm and provides the location of the business.
4. Identifies the Project Manager in your organization (provide address, telephone number, and email address) for future correspondence on projects.

5. Includes the signature of a person authorized to bind the offering organization to the terms of the RFP.
6. Includes Federal tax ID number and State of incorporation.
7. States that the Proposal includes all terms and conditions required by the RFP.
8. Contains a statement certifying that there is no known conflict of interest.

B. CLIENT REFERENCES

Two Page Limit

Provide at least two client references where similar services were provided. Include phone and email contact information.

C. INSURANCE AND PROFESSIONAL SERVICES AGREEMENT REQUIREMENTS

1. PCMC is expecting to enter into a Professional Services Agreement – Cyber Standard with the selected Respondents. A sample of the agreement is provided in **Exhibit "A"** to the RFP. Respondents selected to provide services shall be required to enter into a written agreement in substantially the form as shown in the attached sample agreement which shall be the basic form used to develop the final agreement.

2. If Respondent takes exception to any term or condition set forth in this RFP and/or the sample agreement, said exceptions must be clearly identified in the Proposal. Any inquiries related to indemnification or insurance provisions contained in PCMC'S standard agreement must be submitted to PCMC no later than the RFP submittal deadline. PCMC may, in its sole discretion, consider such inquires. Any changes to PCMC's standard insurance and indemnification provision shall be approved at PCMC's sole discretion.

3. Exceptions or deviations to any of the terms and conditions must be submitted as an attachment accompanying the RFP and identified as "Exceptions." PCMC shall be the sole determiner of the acceptability of any exception. The nature and extent of requested changes to our standard contract (i.e., unwillingness to comply with our insurance/indemnity provision) may count against a Respondent. Such exceptions shall be considered in the evaluation and the award processes.

PART 2 - Technical Response

A. ORGANIZATION & KEY PERSONNEL

Three Page Limit.

Provide the following information about the Respondent's key personnel available to participate in assigned tasks:

1. <u>Organization</u>
   a. Indicate the location of your office and your Project Manager – Describe the proximity of Respondent's project office and Project Manager to Park City.
   b. Discuss key personnel, their qualifications, and the role they will play in providing Water System SCADA Integrator Services.

2. Third Party Personnel
   If Respondent 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.

B. SUMMARY

Two Page Limit.

Summarize your submittal and add any other comments that you feel would make your firm (team) uniquely qualified to participate in this project. In other words, why should we hire your firm (team)?

1. Special Resources. A description of special resources or capabilities your organization could employ on the work that would enhance the value your organization would bring to PCMC. Fiber optic experience, if applicable, should be noted here.

4.0 PROPOSAL EVALUATION PROCESS AND CRITERIA

An evaluation committee, established by PCMC, will review the submitted Proposals and determine which Respondents to select. This section describes the process and criteria by which the evaluation committee will evaluate the Proposals. The evaluation process steps and criteria are as follows:

A. Administrative and Completeness Screening (Mandatory Requirements)

Each Proposal will be screened for compliance with the Administrative Screening Criteria below. The evaluation committee will evaluate each Proposal to determine its responsiveness to these requirements. Proposals that fail or do not fully comply with the Administrative and Completeness Screening Criteria shall be disqualified and eliminated from further evaluation.

1. The Proposal must be received by the exact time and date set and at the stated location for receipt of RFPs.
2. The Proposal must not contain false or intentionally misleading statements or references that do not support an attribute or condition contended by the Respondent.
3. The Proposal must not be intended to mislead PCMC in its evaluation of the Proposal and the attribute, condition, or capability of Respondent.
4. Respondents must not have a conflict of interest as stated in this RFP.
5. By submittal of a signed RFP without submitting proposed changes to the terms of the Professional Services Agreement - Cyber, Respondent indicates acceptance of the terms of the Professional Services Agreement -Cyber.

B. Grounds to Reject a Proposal

In addition to the Administrative Screening Criteria identified above, PCMC reserves the right to reject a Proposal if:

1. The Proposal is unsigned.
2. The Proposal is not prepared in the format described.

3. The Respondent has submitted multiple Proposals.
4. The Proposal does not comply or contains caveats that conflict with the RFP and the variation or deviation is material, or it is otherwise non-responsive.

C. Evaluation of Proposals

The technical evaluation will be based upon a determination by PCMC's evaluation committee members as to how well each Proposal meets PCMC's requirements as presented in this RFP. Each RFP will be evaluated as outlined below.

1. **Proposal Criteria Weighting**

   Proposals will be evaluated by the evaluation committee on the criteria and the corresponding weight factors listed below.

	Maximum Points
A. Proposer Identification and Organization	(35)
B. Insurances and PSA Requirements	(10)
C. Technical Response	(40)
G. Summary	(15)
Maximum Total Points	**(100)**

D. Evaluation of Proposals

The evaluation committee will be comprised of qualified persons, which may include PCMC staff or representatives from other public and private stakeholders. The evaluation committee will open, review, and evaluate all Proposals.

1. Ranking a Proposal
   a. After each Proposal is scored, it will be placed on a list, in rank order, with the highest scoring Proposal placed first and the remainder in descending order based on score.
   b. If Proposals cannot be ranked from the information provided in the Proposal or if additional information or clarification is required, PCMC may request additional information or may invite Respondents submitting the most highly ranked RFPs to interviews.
2. Interviews

   Interviews are not anticipated but may be conducted at PCMC's request.
3. Notice of Selection

   After the Proposal evaluations, the evaluation committee will notify one or more top-scoring Respondent(s) of their selection.

4. Negotiations

   After the issuance of the Notice of Selection, PCMC will begin negotiations with one or more top-ranked Respondent(s) for the final acceptable scope and fee.

   a. If negotiations are not successful, PCMC may terminate the negotiation and enter negotiations with the next highest scoring Respondent, and so on.

   b. Upon successful negotiations with a selected Respondent, PCMC staff will present a recommendation to the City Manager or City Council, as applicable, to enter into an agreement with the selected Respondent.

5. Contract Authorization

   Award of a Professional Services Agreement - Cyber Standard may be subject to approval by the City Council.

E. Procurement Through Other Processes

PCMC reserves the right to acquire additional or alternative water system SCADA Integrator services under any process allowed under PCMC's Procurement Rules.

5.0 GENERAL PROVISIONS

PCMC reserves the right to reject any and all Proposals for any reason.

A. Government Records Access and Management Act.

PCMC will maintain a nonpublic process for the duration of this solicitation in accordance with Government Records Access and Management Act, Title 63G, Chapter 2 of the Utah Code ("GRAMA"). Pursuant to Utah Code § 63G-2-305(6), all records related to this RFP, including but not limited to proposals, evaluation, and selection procedures, and any records created during the evaluation and selection process will remain nonpublic records during the procurement process. After execution of a contract, all submittals will be treated as public records in accordance with the requirements of GRAMA unless otherwise claimed by the Respondent as exempt from disclosure pursuant to Utah Code § 63G-2-309, as amended. The burden of claiming an exemption shall rest solely with each Respondent. Respondent shall submit any materials for which Respondent claims an exemption from disclosure marked as "Confidential" and accompanied by a statement from Respondent supporting the exemption claim. PCMC shall make reasonable efforts to notify Respondent of any GRAMA requests for documents submitted under an exemption claim. Respondent waives any claims against PCMC related to disclosure of any materials pursuant to GRAMA. Please note the following:

   a. Respondent must not stamp all materials confidential. Only those materials for which a claim of confidentiality can be made under GRAMA, such as trade secrets, pricing, non-public financial information, etc., should be stamped.

b. Respondent must submit a letter stating the reasons for the claim of confidentiality for every type of information that is stamped "Confidential." Generally, GRAMA only protects against the disclosure of trade secrets or commercial information that could reasonably be expected to result in unfair competitive injury. Failure to timely submit a written basis for a claim of "Confidential" may result in a waiver of an exemption from disclosure under GRAMA.

c. For convenience, a Business Confidentiality Request Form ("BCR Form") is attached to this RFP as ***Attachment 1***. Respondent must submit a completed BCR Form at the time of submission of any Proposal containing confidential information.

B. Ethics.

By submission of a proposal, Respondent represents and agrees to the following ethical standards:

REPRESENTATION REGARDING ETHICAL STANDARDS: Respondent represents that it has not: (1) provided an illegal gift or payoff to a PCMC officer or employee or former PCMC officer or employee, or his or her relative or business entity; (2) retained any person to solicit or secure this contract upon an agreement or understanding for a commission, percentage, or brokerage or contingent fee, other than bona fide employees of bona fide commercial selling agencies for the purpose of securing business; (3) knowingly breached any of the ethical standards set forth in PCMC's conflict of interest ordinance, Title 3, Chapter 1 of the Park City Code; or (4) knowingly influenced, and hereby promises that it will not knowingly influence, a PCMC officer or employee or former PCMC officer or employee to breach any of the ethical standards set forth in PCMC's conflict of interest ordinance, Title 3, Chapter 1 of the Park City Code.

C. No Representations or Warranty.

It is the responsibility of each Respondent to carefully examine this RFP and evaluate all of the instructions, circumstances and conditions which may affect any proposal. Failure to examine and review the RFP and other relevant documents or information will not relieve Respondent from complying fully with the requirements of this RFP. Respondent's use of the information contained in the RFP is at Respondent's own risk and no representation or warranty is made by PCMC regarding the materials in the RFP.

D. Cost of Developing Proposals.

All costs related to the preparation of the Proposals and any related activities are the sole responsibility of the Respondent. PCMC assumes no liability for any costs incurred by Respondents throughout the entire selection process.

E. Equal Opportunity.

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

F. Proposal Ownership.

All Proposals, including attachments, supplementary materials, addenda, etc., will become the property of PCMC and will not be returned to the Respondent.

G. Modification of RFP.

PCMC reserves the right to cancel or modify the terms of this RFP and/or the project at any time and for any reason preceding the contract execution. PCMC will provide written notice to Respondents of any cancellation and/or modification.

H. Financial Responsibility.

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

I. Local Businesses.

PCMC's policy is to make reasonable attempts to support local businesses by purchasing goods and services through local vendors and service providers, subject to Federal, State, and local procurement laws.

J. Exhibits

Exhibit A:	Park City Municipal Corporation Professional Services Agreement – Cyber Standard
Attachment 1:	Business Confidentiality Form

EXHIBIT "A"
PROFESSIONAL SERVICES AGREEMENT – CYBER STANDARD

This Professional Services Agreement ("**Agreement**") is between **PARK CITY MUNICIPAL CORPORATION**, a Utah municipal corporation ("**PCMC**"), and [insert NAME OF SERVICE PROVIDER], a [insert state of incorporation or formation] [insert "corporation," "limited liability company," or other entity type] (the "**Service Provider**").

PCMC and Service Provider want to enter into an agreement for the Service Provider to perform the services and tasks as specified below.

The parties therefore agree as follows:

ARTICLE 1 – SCOPE OF SERVICES.

A. Scope of Services. Service Provider shall perform the services and tasks identified and designated as Service Provider responsibilities throughout this Agreement and as outlined in **Schedule A** attached to this Agreement ("**Scope of Services**").

Service Provider shall abide by the requirements **in Schedule B** ("**Technology Support, Infrastructure & Security"**) which is attached to this Agreement and incorporated herein.

B. Service Provider Representative. Service Provider designates [insert name of Service Provider representative] as the authorized representative vested with the authority to act on behalf of the Service Provider. Service Provider may change its designated representative by providing written notice to PCMC.

C. PCMC Representative. PCMC designates [insert project manager name] or their designee as its representative who has the authority to act on behalf of PCMC.

ARTICLE 2 – TERM.

This Agreement will become effective as of the date the last party signed it as indicated by the date associated with that party's signature. The term of this Agreement ends at midnight on [insert date in format MM/DD/YYYY] unless terminated sooner or extended as provided in this Agreement.

OPTIONAL: PCMC may at its sole option extend the term of this Agreement for [insert number] additional period(s) of [insert "year(s)" "month(s)" or other time period] each by notifying Service Provider in writing at least thirty days prior to the expiration of this Agreement.

ARTICLE 3 – COMPENSATION, INVOICING, AND PAYMENT.

A. Compensation. For performance of the Scope of Services, PCMC shall pay a total fee in an amount not to exceed $[insert numeric dollar amount]. Any work performed beyond the defined Scope of Services requires a written request from PCMC. Compensation for such additional work shall adhere to the terms outlined in Schedule C, if attached. In the absence of a Schedule C, any compensation for extra work shall be determined based on a mutually agreed-upon written agreement between both parties.

B. Invoicing and Payment. Service Provider shall invoice PCMC on a monthly basis for services completed during that period. PCMC shall pay Service Provider within 30 days of receipt of each invoice. Requests for earlier payment will be considered if a discount is offered for the earlier payment. For services that remain unpaid for a period exceeding 60 days, interest will accumulate at a rate of six percent per annum.

ARTICLE 4 – SERVICE STANDARDS AND COMPLIANCE WITH LAWS.

a. Service Standards. Service Provider shall be responsible for the quality of all services performed by its employees, agents, subcontractors, and all other persons (collectively, "Subcontractors") performing any services under this Agreement. All services shall be executed with competence and in conformity with the standard of care, diligence, and skill typically exercised by professionals within the Service Provider's field.

b. Conformance to Laws. In providing services under this Agreement, Service Provider and its Subcontractors shall comply with all applicable federal, state, PCMC, and other local laws, regulations, and ordinances, including applicable licensure and permit requirements, regulations for certification, operation of facilities, and accreditation, employment laws, and any other standards or criteria described in this Agreement.

c. E-Verify. Service Provider shall register and participate in E-Verify or an equivalent program for each employee employed within the state of Utah if this Agreement is entered into for the physical performance of services within Utah, unless exempted by Utah Code § 63G-12-302. Service Provider shall require that each of its Subcontractors, at every tier, certify under penalty of perjury that each Subcontractor has registered and is participating in E-Verify or an equivalent program, to the extent applicable.

ARTICLE 5 – RECORDS AND INSPECTIONS.

A. Records. Service Provider shall keep any records, documents, invoices, reports, data, information, and all other material regarding matters covered, directly or indirectly, by this Agreement for six years after expiration of this Agreement. This includes everything necessary to properly reflect all expenses related to this Agreement and records of

accounting practices necessary to assure proper accounting of all expenses under this Agreement.

B. Inspection of Records. Service Provider shall make all of the records referenced in this section available for inspection to PCMC, its authorized representatives, the State Auditor, and other government officials authorized to monitor this Agreement by law. Service Provider must permit PCMC or its authorized representative to audit and inspect any data or other information relating to this Agreement. PCMC reserves the right to initiate an audit of the Service Provider's activities concerning this Agreement, at the expense of PCMC, utilizing an auditor selected by PCMC.

C. Government Records Access and Management Act. PCMC is subject to the requirements of the Government Records Access and Management Act, Title 63G, Chapter 2 of the Utah Code ("**GRAMA**"). All materials submitted by Service Provider related to this Agreement are subject to disclosure unless the materials are exempt from disclosure under GRAMA. The burden of claiming an exemption from disclosure rests solely with Service Provider. Any materials for which Service Provider claims an exemption from disclosure based on business confidentiality as provided in Utah Code § 63G-2-309 (or successor provision) must be marked as "Confidential" and accompanied at the time of submission by a statement from Service Provider explaining the basis for the claim. Generally, GRAMA only protects against the disclosure of trade secrets or commercial information that could reasonably be expected to result in unfair competitive injury. PCMC 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 PCMC related to disclosure of any materials pursuant to GRAMA.

ARTICLE 6 – RELATIONSHIP OF PARTIES.

A. Independent Contractor. The parties intend that Service Provider is an independent contractor and not an employee of PCMC. Except as specifically provided in this Agreement, the parties intend that Service Provider has no authority to act on behalf of PCMC.

B. Subcontractor Relationship. The Service Provider shall have full control and authority over performance and activities of its Subcontractors throughout the execution of this Agreement. It is the sole responsibility of Service Provider to ensure that its Subcontractors adhere to the terms and conditions outlined in this Agreement. Furthermore, Service Provider shall bear full responsibility for any actions or omissions of its Subcontractors.

C. Treatment of Assets. Neither party will have an interest in the intellectual property owned or licensed by the other party, unless otherwise agreed by the parties in writing. PCMC

will become the owner of all deliverables, work product, and other materials specifically created by the Service Provider and its Subcontractors under this Agreement.

ARTICLE 7 – INDEMNIFICATION.

Definitions. In this Agreement, the following definitions apply:

(1) "**Indemnifiable Losses**" means the aggregate of Losses and Litigation Expenses.

(2) "**Litigation Expense**" means any reasonable out-of-pocket expense incurred in defending a Proceeding or in any related investigation or negotiation, including court filing fees, court costs, arbitration fees, witness fees, and attorneys' and other professionals' fees and disbursements.

(3) "**Loss**" means any amount awarded in, or paid in settlement of, any Proceeding, including any interest but excluding any Litigation Expenses.

(4) "**Proceeding**" means any investigation, claim, judicial, administrative, or arbitration action or lawsuit, or other cause of action of every kind or character, brought by third parties against PCMC, its agents, employees, or officers, that arises out of this Agreement or the performance of this Agreement by Service Provider or its Subcontractors or subconsultants of any tier, or anyone acting under Service Provider's direction or control, including after the expiration or termination of this Agreement.

Indemnification. Service Provider shall indemnify PCMC and its agents, employees, and officers against all Indemnifiable Losses arising out of a Proceeding, except to the extent the Indemnifiable Losses were caused by the negligence or willful misconduct of PCMC.

Obligation to Defend. Service Provider shall, at its sole cost and expense, defend PCMC and its agents, employees, and officers from and against all Proceedings, provided that Service Provider is not required to defend PCMC from any Proceeding arising from the sole negligence of PCMC or its agents, employees, or officers.

Tender. Service Provider's obligation to defend will arise upon PCMC's tender of defense to Service Provider in writing. If PCMC fails to timely notify Service Provider of a Proceeding, Service Provider will be relieved of its indemnification obligations to the extent that Service Provider was prejudiced by that failure. Upon receipt of PCMC's tender of defense, if Service Provider does not promptly notify PCMC of its acceptance of the defense and thereafter duly and diligently defend PCMC and its agents, employees, and officers, then Service Provider shall pay and be liable for the reasonable costs, expenses, and attorneys' fees incurred in defending the Proceeding and enforcing this provision.

Legal Counsel. To assume the defense, Service Provider must notify PCMC of their intent to do so. Promptly thereafter, Service Provider shall retain independent legal counsel that is reasonably acceptable to PCMC.

Settlement. After Service Provider assumes the defense of a Proceeding, Service Provider may contest, pay, or settle the Proceeding without the consent of PCMC only if that settlement (1) does not entail any admission on the part of PCMC that it violated any law or infringed the rights of any person, (2) provides as the claimant's sole relief monetary damages that are paid in full by Service Provider, and (3) requires that the claimant release PCMC and its agents, employees, and officers from all liability alleged in the Proceeding.

Waiver. Service Provider expressly agrees that the indemnification provision herein constitutes the Service Provider's waiver of immunity under Utah Code § 34A-2-105 for the purposes of this Agreement. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this Agreement. No liability shall attach to PCMC by reason of entering into this Agreement except as expressly provided herein.

No Limitation. The indemnification obligations of this Agreement shall not be reduced by a limitation on the amount or type of damages, compensation, or benefits payable by or for the Service Provider or Subcontractor under workers' compensation acts, disability benefits acts, or other employee benefit acts.

Interpretation. The parties intend that the indemnity and defense provisions in this Article shall be interpreted so as to be enforceable to the fullest extent permitted by law, but nothing herein shall be interpreted to violate public policy.

Environmental Indemnity. Service Provider shall indemnify PCMC, its agents, employees, and officers for any Indemnifiable Losses from a Proceeding arising out of Service Provider's violation of federal, state, or local environmental laws or regulations, and shall include but not be limited to all cleanup and remedial costs, diminution in value of property, and any fines or fees imposed as a result.

ARTICLE 8 – INSURANCE.

At its own cost and expense, Service Provider shall maintain the following mandatory insurance coverage to protect against claims for injuries to persons or property damage that may arise from or relate to the performance of this Agreement by Service Provider, its agents, representatives, employees, or Subcontractors for the entire duration of this Agreement or for such longer period of time as set forth below. Prior to commencing any work, Service Provider shall furnish a certificate of insurance as evidence of the requisite coverage. The certificate of

insurance must include endorsements for additional insured, waiver of subrogation, primary and non-contributory status, and completed operations.

A. Commercial General Liability Insurance. Service Provider shall maintain commercial general liability insurance on a primary and non-contributory basis in comparison to all other insurance, including PCMC's own policies of insurance, for all claims against PCMC. The policy must be written on an occurrence basis with limits not less than $1,000,000 per occurrence and $3,000,000 aggregate for personal injury and property damage. Upon request of PCMC, Service Provider must increase the policy limits to at least the amount of the limitation of judgments described in Utah Code § 63G-7-604, the Governmental Immunity Act of Utah (or successor provision), as calculated by the state risk manager every two years and stated in Utah Admin. Code R37-4-3 (or successor provision).

B. Automobile Liability Coverage. Service Provider shall maintain automobile liability insurance with a combined single limit of not less than $2,000,000 per accident for bodily injury and property damage arising out of the ownership, maintenance, and use of owned, hired, and non-owned motor vehicles. This policy must not contain any exclusion or limitation with respect to loading or unloading of a covered vehicle.

C. Professional Liability Insurance. [Delete if NOT applicable] Service Provider shall maintain professional liability insurance with annual limits not less than $1,000,000 per occurrence. If written on a claims-made basis, Service Provider shall maintain professional liability insurance coverage meeting these requirements for the applicable period of statutory limitation of claims (or statute of repose, if applicable) after completion of the Scope of Services or termination of this Agreement.

D. Workers' Compensation Insurance and Employer's Liability. Service Provider shall maintain workers' compensation insurance with limits not less than the amount required by statute, and employer's liability insurance limits of at least $1,000,000 each accident, $1,000,000 for bodily injury by accident, and $1,000,000 each employee for injury by disease. The workers' compensation policy must be endorsed with a waiver of subrogation in favor of "Park City Municipal Corporation" for all work performed by the Service Provider, its employees, agents, and Subcontractors.

E. Data Breach and Privacy/Cyber Liability Insurance. Service Provider shall maintain data breach and privacy/cyber liability coverage, including coverage for failure to protect confidential information, and failure of the security of the Service Provider's computer systems or the PCMC's systems due to the actions of the Service Provider which results in unauthorized access to the PCMC'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 PCMC's property, including but not limited to money and securities.

F. Technology Errors and Omissions Insurance. Service Provider shall maintain technology errors and omissions insurance with a limit of no less than $5,000,000 for damages arising from computer-related services including but not limited to the following:

- Software services;
- 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.

This policy shall include coverage for third-party fidelity including cyber theft. Data Breach and Privacy / Cyber Liability Insurance and Technology Errors and Omissions insurance may be covered by the same policy.

G. Umbrella/Excess Coverage. The insurance limits required by this section may be met by either providing a primary policy or in combination with umbrella / excess liability policy(ies). To the extent that umbrella/excess coverage is used to satisfy the limits of coverage required hereunder, the terms of such coverage must be following form to, or otherwise at least as broad as, the primary underlying coverage, including amending the "other insurance" provisions as required so as to provide additional insured coverage on a primary and non-contributory basis, and subject to vertical exhaustion before any other primary, umbrella/excess, or any other insurance obtained by the additional insureds will be triggered.

H. Insured Parties. Each policy and all renewals or replacements, except those policies for Professional Liability, and Workers Compensation and Employer's Liability, must name PCMC (and its officers, agents, and employees) as additional insureds on a primary and non-contributory basis with respect to liability arising out of work, operations, and completed operations performed by or on behalf of Service Provider.

I. Waiver of Subrogation. Service Provider waives all rights against PCMC and any other additional insureds for recovery of any loss or damages to the extent these damages are covered by any of the insurance policies required under this Agreement. Service Provider shall cause each policy to be endorsed with a waiver of subrogation in favor of PCMC for all work performed by Service Provider, its employees, agents, and Subcontractors.

J. Quality of Insurance Companies. All required insurance policies must be issued by insurance companies qualified to do business in the state of Utah and listed on the United States Treasury Department's current Department of Treasury Fiscal Services List 570, or having a general policyholders rating of not less than "A-" in the most current available A.M. Best Co., Inc.'s, Best Insurance Report, or equivalent.

K. Cancellation. Should any of Service Provider's required insurance policies under this Agreement be cancelled before the termination or completion of this Agreement, Service Provider must deliver notice to PCMC within 30 days of cancellation. PCMC may request and Service Provider must provide within 10 days certified copies of any required policies during the term of this Agreement.

L. Additional Coverage. Notwithstanding anything to the contrary, if Service Provider has procured any insurance coverage or limits (either primary or on an excess basis) that exceed the minimum acceptable coverage or limits set forth in this Agreement, the broadest coverage and highest limits actually afforded under the applicable policy(ies) of insurance are the coverage and limits required by this Agreement and such coverage and limits must be provided in full to the additional insureds and indemnified parties under this Agreement. The parties expressly intend that the provisions in this Agreement will be construed as broadly as permitted to be construed by applicable law to afford the maximum insurance coverage available under Service Provider's insurance policies.

M. No representation. In specifying minimum Service Providers insurance requirements, PCMC does not represent that such insurance is adequate to protect Service Provider from loss, damage or liability arising from its work. Service Provider is solely responsible to inform itself of types or amounts of insurance it may need beyond these requirements to protect itself.

ARTICLE 9 – NONDISCRIMINATION.

A. Nondiscrimination. Service Provider shall not discriminate against any employee or applicant for employment because of race; ethnicity; color; pregnancy, childbirth, or pregnancy-related conditions; age, if the individual is 40 years of age or older; religion; national origin; disability; sexual orientation; gender identity; or military status.

(1) Policy. Service Provider shall implement an employment nondiscrimination policy, if Service Provider does not already have such a policy, to effectuate the prohibition in this section; and

(2) Subcontractor Flow-Through. Service Provider shall incorporate the foregoing non-discrimination provisions in all subcontracts or assignments under this Agreement and take action as required to ensure full compliance with the provisions of this non-discrimination policy.

ARTICLE 10 – ASSIGNMENT/SUBCONTRACTING.

A. Assignment. Service Provider shall not assign any portion of its performance under this Agreement without PCMC's written consent. Consent must be sought in writing by the Service Provider not less than 30 days before the date of any proposed assignment. PCMC reserves the right to reject assignment without cause. Any purported transfer in violation of this section will be void.

B. Subcontracting. Service Provider shall obtain advance written consent from PCMC for any Subcontractor not identified in the Scope of Services.

ARTICLE 11 – TERMINATION.

A. Convenience**.** Either party may terminate this Agreement for any reason or no reason by giving the other party at least 30 days' prior written notice. This Agreement will terminate at midnight at the end of the 30th day after that notice is effective. Service Provider must be paid its costs, including contract close-out costs, and profit on work performed up to the time of termination, according to the provisions of this Agreement.

B. For Cause. If Service Provider fails to comply with any provision of this Agreement and fails to correct noncompliance within three days of having received written notice, PCMC may immediately terminate this Agreement for cause by providing a notice of termination to Service Provider.

ARTICLE 12 – NOTICES.

A. Notice Addresses. For a notice or other communication to a party under this Agreement to be valid, it must be addressed using the information specified below for that party or any other information specified by that party in a notice delivered in accordance with this section.

To PCMC:

Park City Municipal Corporation
P.O. Box 1480
Park City, UT 84060-1480
Attn: City Attorney's Office
PCMC_Notices@parkcity.org

With a copy to:
- PCMC's Representative pursuant to Article 1.C.
- PCMC's City Recorder at michelle.kellogg@parkcity.org.

To Service Provider:

[Name]
[Address Line 1]
[Address Line 2]
[Email address]

B. Delivery. A notice or other communication under this Agreement will be effective if it is in writing and received by the party to which it is addressed. It will be deemed to have been received as follows: (1) upon receipt as stated in the tracking system of a delivery organization that allows users to track deliveries; (2) when the intended recipient signs for the delivery; (3) when delivered by email to the intended recipient with a read receipt, an acknowledgement of receipt, or an automatic reply.

C. Refusal or Inability to Deliver. If the intended recipient rejects or otherwise refuses to accept delivery, or if it cannot be delivered because of a change of address for which no notice was given, then delivery is effective upon that rejection, refusal, or inability to deliver.

D. Time of Delivery. If a notice or other communication addressed to a party is received after 5:00 p.m. on a business day at the location specified in the address for that party, or on a day that is not a business day, then the notice will be deemed received at 9:00 a.m. on the next business day.

ARTICLE 13 – MISCELLANEOUS PROVISIONS.

A. Entire Agreement. This Agreement constitutes the entire understanding between the parties regarding the subject matter of this Agreement.

B. Modification and Waiver. To be effective, any modification to this Agreement or to the Scope of Services must be in writing and signed by both parties. No waiver under this Agreement will be effective unless it is in writing and signed by the party granting the

waiver (in the case of PCMC, by an individual authorized by PCMC to sign the waiver). A waiver granted on one occasion will not operate as a waiver on other occasions.

C. Timely Performance. Service Provider shall complete the Scope of Services by any applicable deadline stated in this Agreement. Service Provider is liable for all reasonable damages to PCMC incurred as a result of Service Provider's failure to timely perform the Scope of Services required under this Agreement.

D. Governing Law, Jurisdiction, Venue. Utah law governs all adversarial proceedings arising out of this Agreement or the subject matter of this Agreement. As the exclusive means of bringing adversarial proceedings to resolve any dispute arising out of this Agreement or the subject matter of this Agreement, a party may bring such a proceeding in courts of competent jurisdiction in Summit County, Utah.

E. Severability. The parties acknowledge that if a dispute between the parties arises out of this Agreement or the subject matter of this Agreement, it would be consistent with the wishes of the parties for a court to interpret this Agreement as follows: (1) with respect to any provision that it holds to be unenforceable, by modifying that provision to the minimum extent necessary to make it enforceable or, if that modification is not permitted by law, by disregarding that provision; (2) if an unenforceable provision is modified or disregarded in accordance with this section, by holding that the rest of the Agreement will remain in effect as written; (3) by holding that any unenforceable provision will remain as written in any circumstances other than those in which the provision is held to be unenforceable; and (4) if modifying or disregarding the unenforceable provision would result in failure of an essential purpose of this Agreement, by holding the entire Agreement unenforceable.

F. No Non-Party Rights. Nothing in this Agreement is intended to grant rights of any kind to any non-party or create third-party beneficiary rights of any kind.

G. Force Majeure. For purposes of this Agreement, a Force Majeure Event means any event or circumstance, regardless of whether it was foreseeable, that was not caused by that party and that prevents a party from complying with any of its obligations under this Agreement, but a Force Majeure Event will not include any strike or labor unrest, an increase in prices, a change in general economic conditions, or a change of law. A party that is prevented by the occurrence of a Force Majeure Event from performing any one or more obligations under this Agreement will not be liable for any failure or delay in performing those obligations, on condition that the non-performing party uses reasonable efforts to perform. The non-performing party shall promptly notify the other party of the occurrence of a Force Majeure Event and its effect on performance. Thereafter, the nonperforming party shall update the other party as reasonably necessary

regarding its performance. The nonperforming party shall use reasonable efforts to limit damages to the other party and to complete its full performance under this Agreement.

Each party is signing this Agreement on the date stated opposite that party's signature.

PARK CITY MUNICIPAL CORPORATION, a Utah municipal corporation

Date: _____

By: _____
Matt Dias
City Manager

Attest:

_____
City Recorder's Office

Approved as to form:

_____
City Attorney's Office

[insert NAME OF SERVICE PROVIDER]
Tax ID #: _____
PC Business License #: BL_____

Date: _____

By: _____
[insert name of individual signing]
[insert title of individual signing]
An authorized signer

SCHEDULE A – SCOPE OF SERVICES

SCHEDULE B -- TECHNOLOGY SUPPORT, INFRASTRUCTURE & SECURITY

The Information Technology Department is responsible for the administration of this policy. If you have any questions regarding this policy, please contact the Information Technology Department 435-615-5123, 5123@parkcity.org

1. Definitions.

“City Data” / “Information” means any data provided, shared, created or managed by PCMC.

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

“Personally Identifiable Information” or “PII” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (e.g., name, SSN, mailing address, email address, phone number, vehicle plate number, passport number, driver’s license number, medical records).

“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.

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

“Security Breach” means 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” means any Personally Identifiable Information or any information not publicly available (e.g., clients, passwords, financial information, employee information, schedules, technology infrastructure, closed reports, draft notes, etc.).

“Service Provider” means the contract holder that manages employees, contractors or affiliates having access to Park City Municipal Corporation infrastructure or data for specific defined purpose.

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

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

2. 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:

2.1. Sensitive Information (including PII)

Sensitive Information means any Personally Identifiable Information or any information not publicly available. Unauthorized disclosure of this information is not permitted.

2.2. Internal Information

Internal Information is intended for unrestricted use within PCMC, and in some cases within affiliated organizations such as Service Provider business partners for non-sales purposes. 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, most internal electronic mail messages.

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

Unauthorized disclosure of this information is not permitted.

2.3. Public Information

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.

This information may be disclosed outside of Service Provider.

3. Formal Security Policy.

Consistent with the requirements of this Agreement, Service Provider will create and provide to PCMC an information security policy that is approved by Service Provider's management, and published, communicated and agreed to be adhered to by all Service Provider's employees, contractors and affiliates.

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.

4. Asset Management.

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.

Equipment Use While on PCMC Premises: While on PCMC's premises, Service Provider will not connect hardware (physically or via a wireless connection) to PCMC 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 directly or by automated means before use.

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

5. Human Resources Security.

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 a change of assignment.

6. Physical and Environmental Security.

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 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:

Visitors to secure areas shall be supervised.

7. Geographic Data Centers.

Service Provider's data centers shall be 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. 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 shall implement 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.

9. Role Based Access.

Service Provider shall restrict 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.

10. Communications and Operations Management.

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.

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 ensuring 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.

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

Media and Information Disposal. Service Provider will securely and safely dispose of media containing Sensitive Information and maintain a secured disposal log that provides an audit trail of disposal activities.

11. Exchange of Information.

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

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.

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

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

12. Monitoring.

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

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 180 days.

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

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

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

Ensure common configuration and patch management information is maintained.

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.

13. Access Control.

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.

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

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

14. User Responsibilities.

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

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

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

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

15. 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:

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

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

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

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

16. Operating System Access Control.

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

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

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.

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.

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

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

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

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

17. Information Systems Acquisition, Development and Maintenance.

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

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

Employ industry best practice security controls to minimize information dissemination.

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

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

18. Information Security Incident Management.

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

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

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

Notify PCMC 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 PCMC whether or not Sensitive Information was compromised or released to unauthorized parties, the data affected and/or the details of the event or breach.

19. Business Continuity Management.

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

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.

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.

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 PCMC a copy of the same upon Written Request of the City.

Disaster Recovery. Service Provider has appropriate and reasonable disaster recovery measures in place designed to prevent any interruptions in Service to PCMC. 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.

22. Security Assessments.

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 PCMC with execution of a Confidentiality Agreement with Service Provider.

SCHEDULE C – FEE SCHEDULE FOR EXTRA WORK

Note: Any work in addition to or outside the Scope of Services in Schedule A shall be approved in advance in writing by PCMC and shall not exceed the contract price reflected in Article 3 of the Agreement.

Attachment 1

REQUEST FOR PROTECTED STATUS

(Business Confidentiality Claims under Utah's Government Records Access and Management Act ("GRAMA"), Utah Code § 63G-2-309)

I request that the described portion of the record provided to Park City Municipal Corporation be considered confidential and given protected status as defined in GRAMA.

Name: _____
Address: _____

Description of the portion of the record provided to Park City Municipal Corporation that you believe qualifies for protected status under GRAMA (identify these portions with as much specificity as possible) (attach additional sheets if necessary): _____
_____

The claim of business confidentiality is supported by (please check the box/boxes that apply):

( ) The described portion of the record is a trade secret as defined in Utah Code § 13-24-2.

( ) The described portion of the record is commercial or non-individual financial information the disclosure of which could reasonably be expected to result in unfair competitive injury to the provider of the information or would impair the ability of the governmental entity to obtain the necessary information in the future and the interest of the claimant in prohibiting access to the information is greater than the interest of the public in obtaining access.

( ) The described portion of the record would cause commercial injury to, or confer a competitive advantage upon a potential or actual competitor of, a commercial project entity as defined in Utah Code § 11-13-103(4).

REQUIRED: Written statement of reasons supporting a business confidentiality claim as required by Utah Code § 63G-2-305 (1) –(2) (attach additional sheets if necessary):

_____

_____

NOTE: Claimant shall be notified if the portion of the record claimed to be protected is classified as public or if the determination is made that the portion of the record should be disclosed because the interests favoring access outweigh the interests favoring restriction of access. Records claimed to be protected under this business confidentiality claim may not be disclosed until the period in which to bring the appeal expires or the end of the appeals process, including judicial appeal, **unless the claimant, after notice, has waived the claim by not appealing the classification within thirty (30) calendar days.** Utah Code § 63G-2-309(2).

Signature of Claimant: _____

Date: _____