

# EXHIBIT A

## AGREEMENT FOR PROFESSIONAL, TECHNICAL, OR EXPERT SERVICES CONTRACT NO. \_\_\_\_\_ SHORT TITLE OF WORK PROJECT: QSA and AVS Services for PCI-DSS Compliance

This contract is between the City of Portland, acting by and through its Elected Officials, hereafter called "City," and Coalfire Systems, Inc., hereafter called Contractor. The City's Project Manager for this contract Logan Kleier.

### Effective Date and Duration

This contract shall become effective on April 1, 2008 (or on the date at which every party has signed this contract, whichever is later.) This contract shall expire, unless otherwise terminated or extended, on April 1, 2013.

### Statement of Work

- (a) The statement of work is contained in EXHIBIT A attached hereto and by this reference made a part hereof.
- (b) The delivery schedule for the work is identified in EXHIBIT A.

### Consideration

- (a) City agrees to pay Contractor a sum not to exceed \$214,825.00 for accomplishment of the work.
- (b) Interim payments shall be made to Contractor according to the schedule identified in EXHIBIT A.

Terms and conditions listed on pages 2 - 4.

---

### CONTRACTOR DATA, CERTIFICATION, AND SIGNATURE

Name (please print): Coalfire Systems, Inc.

Address: 150 Nickerson Street, Suite 106, Seattle, WA 98109

Social Security #: NA

Federal Tax ID #: 84-1600418 State Tax ID #: NA Business License #697938

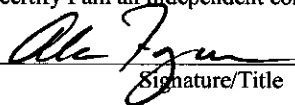
Citizenship: NA Nonresident alien  Yes  No

Business Designation (check one):  Individual  Sole Proprietorship  Partnership  Corporation  
 Limited Liability Co (LLC)  Estate/Trust  Public Service Corp.  Government/Nonprofit

Payment information will be reported to the IRS under the name and taxpayer I.D. number provided above. Information must be provided prior to contract approval. Information not matching IRS records could subject you to 20 percent backup withholding.

I, the undersigned, agree to perform work outlined in this contract in accordance to the terms and conditions (listed on pages 2-4 and made part of this contract by reference) and the statement of work made part of this contract by reference; hereby certify under penalty of perjury that I/my business am not/is not in violation of any Oregon tax laws; hereby certify that my business is certified as an Equal Employment Opportunity Affirmative Action Employer and is in compliance with the Equal Benefits Program as prescribed by Chapter 3.100 of Code of the City of Portland; and hereby certify I am an independent contractor as defined in ORS 670.600.

Approved by the Contractor: \_\_\_\_\_

  
Signature/Title

4/21/08  
Date

---

### CITY OF PORTLAND SIGNATURES

Approved by Mayor or Commissioner: \_\_\_\_\_

Elected Official or Delegate

Date

Approved by City Auditor: \_\_\_\_\_

City Auditor

Date

Approved as to Form  
by City Attorney: \_\_\_\_\_

Office of City Attorney

Date

**EXHIBIT A**  
**CITY OF PORTLAND**  
**STANDARD CONTRACT PROVISIONS FOR**  
**PROFESSIONAL, TECHNICAL & EXPERT SERVICES (MANDATORY PROVISIONS)**

**1. Access to Records**

The Contractor shall maintain, and the City of Portland ("City") and its duly authorized representatives shall have access to the books, documents, papers, and records of the Contractor which are directly pertinent to the specific contract for the purpose of making audit, examination, excerpts, and transcripts for a period of three years after final payment. Copies of applicable records shall be made available upon request. Payment for cost of copies is reimbursable by the City.

**2. Audits**

(a) The City, either directly or through a designated representative, may conduct financial and performance audits of the billings and services specified in this agreement at any time in the course of the agreement and during the three (3) year period established by section 1, **Access to Records**. Audits will be conducted in accordance with generally accepted auditing standards as promulgated in Government Auditing Standards by the Comptroller General of the United States General Accounting Office.

(b) If an audit discloses that payments to the Contractor were in excess of the amount to which the Contractor was entitled, then the Contractor shall repay the amount of the excess to the City.

(c) If any audit shows performance of services is not efficient in accordance with Government Auditing Standards, or that the program is not effective in accordance with Government Auditing Standards, the City may pursue remedies provided under section 5, **Early Termination of Agreement** and section 7, **Remedies**.

**3. Effective Date and Duration**

The passage of the contract expiration date (as recorded on reverse side) shall not extinguish, prejudice, or limit either party's right to enforce this contract with respect to any default or defect in performance that has not been cured.

**4. Order of Precedence**

This contract consists of the terms and conditions of this contract, the Request for Proposals (RFP) issued by the City, if any, and the Contractor's proposal in response to the RFP. In the event of any apparent or alleged conflict between these various documents, the following order of precedence shall apply to resolve the conflict: a) amendments to this agreement signed by both parties b) this contract's terms and conditions, c) the City's RFP, and cd the Contractor's proposal in response to the RFP.

**5. Early Termination of Agreement**

(a) The City and the Contractor, by mutual written agreement, may terminate this Agreement at any time.

(b) The City, on thirty (30) days written notice to the Contractor, may terminate this Agreement for any reason deemed appropriate in its sole discretion.

(c) Either the City or the Contractor may terminate this Agreement in the event of a breach of the Agreement by the other. Prior to such termination, however, the party seeking the termination shall give to the other party written notice of the breach and of the party's intent to terminate. If the party has not entirely cured the breach within fifteen (15) days of the notice, then the party giving the notice may terminate the Agreement at any time thereafter by giving a written notice of termination.

**6. Payment on Early Termination**

(a) In the event of termination under subsection 5(a) or 5(b), **Early Termination of Agreement** hereof, the City shall pay the Contractor for work performed in accordance with the Agreement prior to the termination date.

(b) In the event of termination under subsection 5(c), **Early Termination of Agreement** hereof, by the Contractor due to a breach by the City, then the City shall pay the Contractor as provided in subsection (a) of this section.

(c) In the event of termination under subsection 5(c), **Early Termination of Agreement** hereof, by the City due to a breach by the Contractor, then the City shall pay the Contractor as provided in subsection (a) of this section, subject to set off of excess costs, as provided for in section 7(a), **Remedies**.

(d) In the event of early termination all of the Contractor's work product will become and remain property of the City.

**7. Remedies**

(a) In the event of termination under subsection 5(c), **Early Termination of Agreement**, hereof, by the City due to a breach by the Contractor, then the City may complete the work either itself, by agreement with another contractor or by a combination thereof. In the event the cost of completing the work exceeds the remaining unpaid balance of the total compensation provided under this contract, then the Contractor shall pay to the City the amount of the reasonable excess.

(b) The remedies provided to the City under section 5, **Early Termination of Agreement** and section 7, **Remedies** for a breach by the Contractor shall not be exclusive. The City also shall be entitled to any other equitable and legal remedies that are available.

(c) In the event of breach of this Agreement by the City, then the Contractor's remedy shall be limited to termination of the Agreement and receipt of payment as provided in section 5(c), **Early Termination of Agreement** and section 6(b), **Payment on Early Termination** hereof.

**8. Subcontracts and Assignment**

Contractor shall not subcontract, assign or transfer any of the work scheduled under this agreement, without the prior written consent of the City. Notwithstanding City approval of a subcontractor, the Contractor shall remain obligated for full performance hereunder, and the City shall incur no obligation other than its obligations to the Contractor hereunder. The Contractor agrees that if subcontractors are employed in the performance of this Agreement, the Contractor and its subcontractors are subject to the requirements and sanctions of ORS Chapter 656, Workers' Compensation.

## EXHIBIT A

### 9. Compliance with Applicable Law

In connection with its activities under this Agreement, Contractor shall comply with all applicable federal, state and local laws and regulations including the City's Equal Benefits Ordinance and its administrative rules, all of which are incorporated by this reference. Failure to comply with the Ordinance permits the City to impose sanctions or require remedial actions as stated in Section 13.1 of the administrative rules. Contractor shall complete Exhibit B, Independent Contractor/Workers' Compensation Insurance Questionnaire, which is attached hereto and by this reference made a part hereof.

#### 9a. Indemnity - Claims for Other than Professional Liability

Contractor shall defend, save, and hold harmless the City of Portland, its officers, agents, and employees, from all claims, suits, or actions of whatsoever nature, including intentional acts, resulting from or arising out of the activities of Contractor or its subcontractors, agents or employees under this agreement.

#### 9b. Indemnity - Claims for Professional Liability

Contractor shall defend, save, and hold harmless the City of Portland, its officers, agents, and employees, from all claims, suits, or actions arising out of the professional negligent acts, errors or omissions of Contractor or its subcontractors and sub-consultants, agents or employees in performance of professional services under this agreement.

#### 9c. Indemnity - Standard of Care

If Contractor's services involve engineering or consulting, the standard of care applicable to Contractor's service will be the degree of skill and diligence normally employed by professional engineers or consultants performing the same or similar services at the time such services are performed. Contractor will re-perform any services not meeting this standard without additional compensation.

### 10. Insurance

Exhibit C is hereby referenced and made a part of this contract.

### 11. Ownership of Work Product

All work products produced by the Contractor under this contract is the exclusive property of the City. "Work product" shall include but not be limited to research, reports, computer programs, manuals, drawings, recordings, photographs, artwork and any data or information in any form; the Contractor and the City intend that such work product shall be deemed "work made for hire" of which the City shall be deemed the author. If for any reason a work product is deemed not to be a "work made for hire," the Contractor hereby irrevocably assigns and transfers to the City all right, title and interest in such work product, whether arising from copyright, patent, trademark, trade secret, or any other state or federal intellectual property law or doctrines. Contractor shall obtain such interests and execute all documents necessary to fully vest such rights in the City. Contractor waives all rights relating to work product, including any rights arising under 17 USC 106A, or any other rights of authorship, identification or approval, restriction or limitation on use or subsequent modifications. If the Contractor is an architect, the work product is the property of the Contractor-Architect, and by execution of this contract, the Contractor-Architect grants the City an exclusive and irrevocable license to use that work product.

### 12. Nondiscrimination

Contractor agrees to comply with all applicable requirements of federal and state civil rights and rehabilitation statutes, rules, and regulations. Contractor also shall comply with the Americans With Disabilities Act of 1990 (Pub L. No. 101-336) including Title II of that Act, ORS 659.425, and all regulations and administrative rules established pursuant to those laws.

### 13. Successors in Interest

The provisions of this contract shall be binding upon and shall inure to the benefit of the parties hereto, and their respective successors and approved assigns.

### 14. Severability

The parties agree that if any term or provision of this contract is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and provisions shall not be affected, and the rights and obligations of the parties shall be construed and enforced as if the contract did not contain the particular term or provision held to be invalid.

### 15. Waiver

The failure of the City to enforce any provision of this contract shall not constitute a waiver by the City of that or any other provision.

### 16. Errors

The Contractor shall perform such additional work as may be necessary to correct errors in the work required under this contract without undue delays and without additional cost.

### 17. Governing Law

The provisions of this contract shall be construed in accordance with the provisions of the laws of the State of Oregon, without reference to its conflict of laws provisions. Any action or suits involving any question arising under this contract must be brought in the appropriate court in Multnomah County Oregon. Any litigation between the City and Vendor arising under this Contract or out of work performed under this Contract shall occur, if in the state courts, in the Multnomah County Circuit Court, and if in the federal courts, in the United States District Court for the District of Oregon.

## EXHIBIT A

### 18. Amendments

All changes to this contract, including changes to the scope of work and contract amount, must be made by written amendment and approved by the Purchasing Agent to be valid. Any amendment that increases the original contract amount by more than 25% must be approved by the City Council to be valid.

### 19. Business License

The Contractor shall obtain a City of Portland business license as required by PCC 7.02 prior to beginning work under this Agreement. The Contractor shall provide a business license number in the space provided on page one of this Agreement. Additionally, the Contractor shall pay all fees or taxes due under the Business License Law and the Multnomah County Business Income Tax (MCC Chapter 12) during the full term of this contract. Failure to be in compliance may result in payments due under this contract to be withheld to satisfy amount due under the Business License Law and the Multnomah County Business Income Tax Law.

### 20. Prohibited Interest

(a) No City officer or employee during his or her tenure or for one year thereafter shall have any interest, direct or indirect, in this Agreement or the proceeds thereof.

(b) No City officer or employee who participated in the award of this Agreement shall be employed by the Contractor during the period of the Agreement.

### 21. Payment to Vendors and Subcontractors

The Contractor shall timely pay all suppliers, lessors and contractors providing it services, materials or equipment for carrying out its obligations under this Agreement. The Contractor shall not take or fail to take any action in a manner that causes the City or any materials that the Contractor provides hereunder to be subject to any claim or lien of any person without the City's prior written consent.

### Merger Clause

THIS CONTRACT AND ATTACHED EXHIBITS CONSTITUTES THE ENTIRE AGREEMENT BETWEEN THE PARTIES. NO WAIVER, CONSENT, MODIFICATION, OR CHANGE OF TERMS OF THIS CONTRACT SHALL BIND EITHER PARTY UNLESS IN WRITING AND SIGNED BY BOTH PARTIES. SUCH WAIVER, CONSENT, MODIFICATION, OR CHANGE IF MADE, SHALL BE EFFECTIVE ONLY IN SPECIFIC INSTANCES AND FOR THE SPECIFIC PURPOSE GIVEN. THERE ARE NO UNDERSTANDINGS, AGREEMENTS, OR REPRESENTATIONS, ORAL OR WRITTEN, NOT SPECIFIED HEREIN REGARDING THIS CONTRACT. CONTRACTOR, BY THE SIGNATURE OF ITS AUTHORIZED REPRESENTATIVE, HEREBY ACKNOWLEDGES THAT HE OR SHE HAS READ THIS CONTRACT, UNDERSTANDS IT AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.

### OPTIONAL PROVISIONS (selected by City Project Manager)

### 22. Arbitration: / / Not Applicable / / Applicable (consult with City Attorney's Office before finalizing as applicable)

(a) Any dispute arising out of or in connection with this Agreement, which is not settled by mutual agreement of the Contractor and the City within sixty (60) days of notification in writing by either party, shall be submitted to an arbitrator mutually agreed upon by the parties. In the event the parties cannot agree on the arbitrator, then the arbitrator shall be appointed by the Presiding Judge (Civil) of the Circuit Court of the State of Oregon for the County of Multnomah. The arbitrator shall be selected within thirty (30) days from the expiration of the sixty (60) day period following notification of the dispute. The arbitration, and any litigation arising out of or in connection with this Agreement, shall be conducted in Portland, Oregon, shall be governed by the laws of the State of Oregon, and shall be as speedy as reasonably possible. The applicable arbitration rules for the Multnomah County courts shall apply unless the parties agree in writing to other rules. The arbitrator shall render a decision within forty-five (45) days of the first meeting with the Contractor and the City. Insofar as the Contractor and the City legally may do so, they agree to be bound by the decision of the arbitrator.

(b) Notwithstanding any dispute under this Agreement, whether before or during arbitration, the Contractor shall continue to perform its work pending resolution of a dispute, and the City shall make payments as required by the Agreement for undisputed portions of work.

### 23. Progress Reports: / / Applicable / / Not Applicable

The Contractor shall provide monthly progress reports to the Project Manager. If applicable, Exhibit A should list what information the Contractor must include in monthly progress reports.

### 24. Contractor's Personnel: / / Applicable / / Not Applicable

The Contractor shall assign the following personnel to do the work in the capacities designated: If applicable, list selected personnel in Exhibit A. The Contractor shall not change personnel assignments without the prior written consent of the City.

### 25. Subcontractors: / / Applicable / / Not Applicable

The Contractor shall assign the following subcontractors to perform work in the capacities designated: If applicable, list selected subcontractors in Exhibit A. The Contractor shall not change subcontractor assignments without the prior written consent of the City.

### IT PROVISIONS

26. Conflict of Interest. Contractor warrants it has no present interest and shall not acquire any interest that would conflict in any manner with its duties and obligations under the Agreement.

27. Return of Parties' Property. When the Agreement or any Task/Change Order placed pursuant to the Agreement is terminated or expired, each Party shall return to the other all papers, materials, and properties of the other Party then in its possession. The City will retain one (1) copy of the documentation for the express purposes of public record archiving.

## EXHIBIT A

**28. Notice of Change in Financial Condition.** Contractor must maintain a financial condition commensurate with the requirements of the Agreement. If, during the Agreement, Contractor experiences a change in its financial condition which may adversely affect its ability to perform, or changes the ownership or control, the City shall be immediately notified in writing. Failure to notify the City of such a change in financial condition or change in ownership or control is sufficient grounds for terminating the Agreement.

**29. Confidentiality.**

"City Confidential Information" means any information, in any form or media, including verbal discussions, whether or not marked or identified by the City, which is reasonably described by one or more of the following categories of information: (1) financial, statistical, personnel, human resources data or Personally Identifiable Information as described in the Oregon Consumer Identity Theft Protection Act of 2007; (2) business plans, negotiations, or strategies; (3) unannounced pending or future products, services, designs, projects or internal public relations information; (4) trade secrets, as such term is defined by ORS 192.501(2) and the Uniform Trade Secrets Act ORS 646.461 to 646.475; (5) Exempt per ORS 192.501 and/or ORS 192.502 (6) attorney/client privileged communications, (7) exempt per federal laws (including but not limited to Copyright, HIPPA) and (7) information relating to or embodied by designs, plans, configurations, specifications, programs, or systems developed for the benefit of the City including without limitation, data and information systems, any software code and related materials licensed or provided to the City by third parties; processes; applications; codes, modifications and enhancements thereto; and any work products produced for the City.

Maintenance of Confidentiality. Contractor shall treat as confidential any City Confidential Information that has been made known or available to Contractor or that Contractor has received, learned, heard or observed; or to which Contractor has had access. Contractor shall use Confidential Information exclusively for the City's benefit and in furtherance of the goods and/or services provided by Contractor. Except as may be expressly authorized in writing by the City, in no event shall Contractor publish, use, discuss or cause or permit to be disclosed to any other person such Confidential Information. Contractor shall (1) limit disclosure of the Confidential Information to those directors, officers, employees and agents of Contractor who need to know the Confidential Information in connection with the City Project/Network, (2) exercise reasonable care with respect to the Confidential Information, at least to the same degree of care as Contractor employs with respect to protecting its own proprietary and confidential information, and (3) return immediately to the City, upon its request, all materials containing Confidential Information, in whatever form, that are in Contractor's possession or custody or under its control. Contractor is expressly restricted from and shall not use Confidential intellectual property of the City without the City's prior written consent.

Scope. This Agreement shall apply to all City Confidential Information previously received, learned, observed, known by or made available to Contractor. This Agreement shall not apply to Confidential Information which (1) is or later becomes part of the public domain without breach of this Agreement and through no wrongful act of Contractor, (2) Contractor rightly receives from a third party, or (3) was developed independently by and was reduced to writing by Contractor prior to the earlier of the date of this Agreement or the date of any access or exposure to any Confidential Information. Contractor's obligations under this Agreement shall survive termination.

Equitable Remedies. Contractor acknowledges that unauthorized disclosure of City Confidential Information or misuse of the City System or Network will result in irreparable harm to the City. In the event of a breach or threatened breach of this Agreement, the City may obtain equitable relief prohibiting the breach, in addition to any other appropriate legal or equitable relief.

Contractor's Confidential Information. During the term of the Agreement, Contractor may disclose to the City, certain confidential information pertaining to Contractor's business ("Confidential Information"). Contractor shall be required to mark "CONFIDENTIAL" with a restrictive legend or similar marking. If CONFIDENTIAL is not clearly marked or cannot be marked with a restrictive legend or similar marking or is disclosed either orally or by visual presentation, Contractor shall identify the Confidential Information at the time of disclosure or within a reasonable time thereafter. The City shall not be deemed to have breached this Section if (a) Confidential Information later becomes part of the public domain through no act or omission of the City; (b) is required to be disclosed under operation of law; or (c) the City lawfully receives Confidential Information from a third party with no breach of any duty of confidentiality.

**30. Public Records Request.** Contractor acknowledges that the City of Portland is subject to the Oregon Public Records Act and Federal law. Third persons may claim that the Confidential Information Contractor submits to the City hereunder may be, by virtue of its possession by the City, a public record and subject to disclosure pursuant to the Oregon Public Records Law. Subject to the following conditions, the City agrees not to disclose any information Contractor submits to the City that includes a written request for confidentiality and as described above, specifically identifies the information to be treated as Confidential. The City's commitments to maintain certain information confidential under this agreement are all subject to the constraints of Oregon and federal laws. Within the limits and discretion allowed by those laws, the City will maintain the confidentiality of information.

**31. Security.** Contractors providing or having access to Software which contains personally identifiable information must maintain and demonstrate compliance with the following:

31.1 Payment Card Industry- Data Security Standard (PCI-DSS). The most current version is 1.1. These standards are maintained at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

31.2 Effective January 1, 2008, notification provisions of the Oregon Consumer Identity Theft Protection Act of 2007.

**EXHIBIT A**

31.3 City of Portland, Bureau of Technology Services- Security Standards. Specifically Contractors must comply with Technology Services, Information Security Administrative Rules 2.01, 2.02, 2.08, 2.12 and 2.15. These rules are located at: <http://www.portlandonline.com/auditor/index.cfm?c=26821>

31.4 Additionally, Contractors who are third party providers of software which processes and/or interacts with credit card account numbers on behalf of the City or who have access to data held on such software must maintain and demonstrate compliance with the following:

Payment Card Industry- Data Security Standard (PCI-DSS). The most current version is 1.1. These standards are maintained at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

**32. Survival.** All obligations relating to confidentiality; indemnification; publicity; proprietary rights; limitation of liability; and obligations to make payments of amounts that become due under this Agreement prior to termination (except that payments for services not performed by the date of termination shall be prorated) shall survive the termination or expiration of this Agreement and shall, to the extent applicable, remain binding and in full force and effect for the purposes of the ongoing business relationship by and between Contractor and the City. Nothing in this Agreement shall alter, modify, or supersede the content and survival of such provisions, except as otherwise expressly agreed to in writing by the Parties and with the prior written approval of the City Attorney's office.

# EXHIBIT A

## AGREEMENT FOR PROFESSIONAL, TECHNICAL, OR EXPERT SERVICES EXHIBIT A

### Statement of the Work and Payment Schedule

#### **Payment Card Industry- Data Security Standard (PCI-DSS) – Contract SOW between the City of Portland and Coalfire Systems.**

#### **I. COALFIRE SYSTEMS - SCOPE OF WORK (SOW)**

Coalfire Systems (hereinafter identified as “Coalfire”) will provide the City of Portland, Bureau of Technology Services (BTS):

- A PCI Report on Compliance (ROC) assessment from a certified Qualified Security Assessor (QSA) to baseline the City’s full and current compliance status of three distinct payment platforms operated by the City, including:
  - BTS’ Payment Gateway
  - Parks & Recreation Bureau’s on-line class registration systems, and
  - Office of Management and Finance’s Smart Park facilities
- Remediation guidance to supplement the ROC in the form of a Gap Analysis including policy templates and remediation cost estimates
- Quarterly network scans for the active, external facing IP addresses within the above referenced platforms payment card environments (PCE)

#### **Report on Compliance**

Coalfire conducts the ROC through the following project tasks:

1. Charter Meeting
2. Pre-Assessment
3. ROC assessment
4. Analysis & Reporting
5. Presentation & Debrief Meeting

#### ***Task 1 Charter Meeting***

The project will be initiated with a formal kick off meeting, referred to as the Charter. The Charter re-states objectives and aligns the City and Coalfire team members to their specific roles and responsibilities, communication methods, resource availability, and schedules.

During the Charter, Coalfire will request documentation from the City relating to policies, standards, procedures, organizational charts, and other PCI specific diagrams not previously provided.

#### ***Task 2 Pre-Assessment***

Coalfire will conduct a thorough documentation review of PCI-required elements, including documentation covering existing controls, processes, architectural diagrams, card transaction and data flow, general business plans, policies, and procedures. To supplement and validate the documentation review, Coalfire will interview City business units and process managers involved in the payment card environment (PCE) for the three distinct platforms. Coalfire and the City will also inventory payment card systems and document the supporting controls and business processes. The net result of this project task is a defined PCE which ensures appropriate scoping for Task 3 services.

Upon completion, the pre-assessment task templates shall be established, testing sample sizes determined and on-site testing dates scheduled.

## EXHIBIT A

**Work products (Task 2):** There are no written deliverables for this project task, however, Coalfire shall notify the City in writing when it has completed Task 2.

**Project Duration (Task 2):** It is estimated that Task 2 activities will be completed over the course of approximately two weeks, provided reasonable access is allowed to City staff and information related to this task.

### *Task 3 ROC Assessment*

Testing and validation is required to complete the ROC and identify control compliance and non-compliance to the PCI-DSS. Only applicable controls that are part of the PCE assessment scope are subject to testing.

Through a combination of interviews, observations, control performance, and technical testing, Coalfire shall complete the assessment according to PCI ROC testing procedures.

Details regarding QSA security auditing procedures to the PCI DSS may be downloaded at: [www.pcisecuritystandards.org/pdfs/pci\\_audit\\_procedures\\_v1-1.pdf](http://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf)

**Work products (Task 3):** During this project task, test data is collected. There are no specific written deliverables for project Task 3. The test data shall be reviewed and the evidence and conclusions presented in the deliverables associated with project Task 4, the Report on Compliance (ROC), and the Gap Analysis.

**Project Duration (Task 3):** It is estimated that Task 3 activities will be performed over the course of five business days, provided reasonable access is allowed to City staff and information related to this task.

### *Task 4 Analysis & Reporting*

Based on the assessment findings, Coalfire shall complete the Report on Compliance (ROC). The ROC will be presented to the City in draft form and amendments submitted before the ROC is finalized. Any objections or suggested amendments to the ROC shall be provided in writing to Coalfire within 30 days of the delivery of the ROC. The ROC is the primary report required by the card associations to demonstrate compliance for Level 1 merchants. The ROC will be presented to the City in a PCI-compliant format and the City may elect to pass the ROC on to Wells Fargo Bank.

If compliance gaps are identified, a Gap Analysis report shall be presented to the City. The Gap Analysis identifies areas of non-compliance and reports on the level of risk associated with each compliance gap. The Gap Analysis provides details regarding the recommended remediation activities, level of urgency, and budgetary estimates for each activity. The Gap Analysis supplements the ROC and is intended to be used by City management and staff to manage progress towards compliance. The report is also intended to be passed on to the City's acquirer, by the City, to demonstrate the City's commitment to PCI and the City's estimated timelines to deploy the required controls to attain compliance.

As a deliverable, Coalfire will provide City staff with PCI-compliant policy templates that the City may customize to fit their unique business model.

**Work Products (Task 4):** There are three deliverables resulting from the ROC. They include:

- Report on Compliance
- Gap Analysis
- Policy Templates

**Project Duration (Task 4):** It is estimated that Task 4 activities will be completed within two weeks of completion of Task 3 activities.



## EXHIBIT A

### **Task 5 Presentation & Debrief Meeting**

Coalfire will provide an executive presentation to appropriate City managers (IT, Finance) involved in the City's PCI initiative. This meeting will detail Coalfire's findings and serve as an opportunity to clearly explain Coalfire's findings, areas of risk being introduced to the City, and the City's existing controls program alignment to the PCI DSS.

**Work Products (Task 5):** The City will receive a PowerPoint presentation.

**Project Duration (Task 5):** Coalfire will work with the City to conduct the presentation at a time that is mutually agreeable, preferably one week after Task 4 activities conclude.

### **Quarterly Network Scans**

Over the course of four calendar quarters, Coalfire will provide required network scans that meet the scanning requirements for merchants to the City.

Coalfire will schedule scans with IT staff at a time convenient to operations and follow PCI scanning procedures and report formatting. Remediation advice for found vulnerabilities shall be provided to the City along with raw data from the scan results. Vulnerabilities identified as Urgent, Critical or High will be resolved to produce a successful scan report. Scan reports will provide details regarding identified vulnerabilities, vulnerability ratings, and remediation recommendations to address identified vulnerabilities.

The vulnerabilities will be classified in accordance with PCI Security Scanning requirements and are presented below:

Level	Severity	Description
	HIGH	Trojan horses, file read and write exploit, remote command execution
		Potential Trojan Horses, file read exploit
		Limited exploit of read, directory browsing and DoS
		Sensitive Information can be obtained by hackers on configuration
		Configuration information can be obtained by unauthorized users

**Work Products (Quarterly Scans):** Deliverables presented quarterly include:

- *Detailed Scan Results:* This report is automatically generated by most scan tools. This report details each IP scanned and associated vulnerabilities, if any. Also included in the Detailed Scan Results report is an overview of all IP's scanned, along with their vulnerability rating.
- *Vulnerability Tracking Report:* This is intended to supplement the Detailed Scan Results report and is designed to assist the City with the identification of vulnerabilities by hosts and to ensure that an efficient and effective remediation plan is executed.
- *PCI Scan Report:* This report is an abbreviated version of the Detailed Scan Results report and is intended to be passed on to the City's acquiring bank or associated business partners. This report details the full IP assessment scope, each IP's vulnerability score, and a high-level review of any prevalent weaknesses or vulnerabilities.

## EXHIBIT A

### Payment Schedule

The City of Portland shall pay Coalfire for work performed according to the following payment schedule. Tasks 1-5 and the quarterly scans listed below are performed on an annual basis for the length of the contract.

Project Task	Milestones	Price
<b>Task 1 - Charter Meeting/Project Management</b>	1. Establish Project Portal 2. Conduct Charter Meeting 3. Provide the City with a formal document request	\$3,000
<b>Task 2 – Pre-Assessment</b>	1. Review documents, diagrams and policies 2. Map the City’s Payment Card Environment (PCE) 3. Document supporting controls and business processes 4. Establish templates and testing sample sizes 5. Coordinate Task 3 schedules	\$6,750
<b>Task 3 – ROC Assessment</b>	1. On-site interviews, observation, control performance and technical tests	\$14,750
<b>Task 4 – Analysis &amp; Reporting</b>	1. Draft Report on Compliance is presented 2. Final Report on Compliance is presented and accepted by the City 3. Gap Analysis is presented 4. Policy Templates are presented 5. Coordinate Task 5 schedule	\$10,250
<b>Task 5 - Presentation and Debrief Meeting</b>	1. Presentation to City management	\$2,750
<b>Quarterly Scans</b>	1. First Quarterly Scan Reports are posted to the Project Portal	\$866.25
	2. Second Quarterly Scan Reports are posted to the Project Portal	\$866.25
	3. Third Quarterly Scan Reports are posted to the Project Portal	\$866.25
	4. Fourth Quarterly Scan Reports are posted to the Project Portal	\$866.25
<b>Project Services Subtotal</b>		<b>40,965</b>
<b>Maximum Reimbursable Travel Expenses**</b>		<b>\$2,000</b>
<b>Extended Fixed Project Fees</b>		<b>\$42,965</b>

- Coalfire will invoice monthly for project tasks completed. Payment terms shall be Net 30 according to the following schedule and will not exceed \$42,965, unless otherwise authorized by the City.
  1. (Task 1) Approximately 1-4 weeks after completion \$3,000 shall be invoiced.
  2. (Task 2) Approximately 1-4 weeks after completion \$6,750 shall be invoiced.
  3. (Task 3) Approximately 1-4 weeks after completion \$14,750 shall be invoiced.
  4. (Task 4) Approximately 1-4 weeks after completion \$10,250 shall be invoiced\*.
  5. (Task 5) Approximately 1-4 weeks after completion \$2,750 shall be invoiced.
  6. (Quarterly Scan 1) Approximately 1-4 weeks after completion \$866.25 shall be invoiced
  7. (Quarterly Scan 2) Approximately 1-4 weeks after completion \$866.25 shall be invoiced
  8. (Quarterly Scan 3) Approximately 1-4 weeks after completion \$866.25 shall be invoiced
  9. (Quarterly Scan 4) Approximately 1-4 weeks after completion \$866.25 shall be invoiced

## EXHIBIT A

\*Payment for Task 4 services shall be contingent on the City's acceptance of the ROC, which shall not be unduly withheld by the City.

\*\*Travel costs will be billed monthly and will be based on actual incurred travel costs up to a maximum of \$2,000.

\*\*\*Multiple project tasks may be completed in the same month, in which case they will appear on the same invoice.

### CONTRACTOR PERSONNEL

The Contractor shall assign the following personnel to do the work in the capacities designated:

NAME	ROLE ON PROJECT
Harley Rinerson	Executive Sponsor
Tom McAndrew	Project Lead
Deepa Saldanha	Project Support
Steven Weil	Project Support

### SUBCONTRACTORS

The Contractor shall assign the following subcontractors to perform work in the capacities designated:

NAME	ROLE ON PROJECT
None	

The City will enforce all diversity in workforce and Minority, Women and Emerging Small Business (M/W/ESB) subcontracting commitments submitted by the Contractor in its Proposal. The Contractor shall submit a Monthly Subconsultant Payment and Utilization Report (Exhibit A1 attached hereto) reporting ALL subcontractors employed in the performance of this agreement.

### COMPENSATION

Payment shall be issued by the City net thirty (30) days from receipt and acceptance of a proper invoice from Contractor. Contractor invoices must contain the Contractor's name and address; invoice number; date of invoice; Agreement number and date; description of goods or services; quantity, unit price, (where appropriate), and total amount; and the title and phone number of the responsible official to whom payment is to be sent.

EXHIBIT A

MONTHLY SUBCONSULTANT PAYMENT AND UTILIZATION REPORT

- 1. Solicitation No. \_\_\_\_\_
- 2. Contract No. \_\_\_\_\_
- 3. Prime Consultant \_\_\_\_\_
- 4. Contract Amount \_\_\_\_\_
- 5. Report Dates: Beginning \_\_\_/\_\_\_/\_\_\_ Ending Dates \_\_\_/\_\_\_/\_\_\_
- 6. Project Name \_\_\_\_\_
- 7. Progress Report No. \_\_\_\_\_

8 ALL SUBCONSULTANT NAMES APPEARING ON ORIGINAL FIRST-TIER SUBCONSULTANT DISCLOSURE	9 ORIGINAL SUBCONSULTANT AMOUNT (\$)	10 AMENDED SUBCONSULTANT AMOUNT (\$)	11 PAYMENT AMOUNTS AND DATES MADE FOR MONTH (\$)	12 TOTAL PAYMENTS TO DATE
None				

SUBCONSULTANTS ADDED AFTER PROJECT AWARD (Must be EEO Certified with the City of Portland)\*

13 SUBCONSULTANT NAME (LIST ANY SUBCONSULTANTS NOT ABOVE)	14 NATURE OF WORK	15 STATUS MBE, ESB	16 SUBCONSULTANT AMOUNT	17 PAYMENT AMOUNTS AND DATES MADE FOR MONTH (\$)	18 TOTAL PAYMENTS TO DATE
None					

\*CHANGES TO CONTRACT: Before replacing, substituting, or adding any subcontractor, please contact the PTE Compliance Specialist

Please note: Explanations and additional instructions for completing this report are on the reverse side.

IT IS HEREBY CERTIFIED THAT THE ABOVE LISTED FIRMS HAVE BEEN UTILIZED BY OUR FIRM IN THE AMOUNTS REPRESENTED ABOVE AND THAT THE INFORMATION CONTAINED HEREIN IS COMPLETE AND ACCURATE.

Authorized Signature of Consultant Representative \_\_\_\_\_ Date \_\_\_\_\_

Submit with invoice by the 15<sup>th</sup> of the month to the City's Project Manager AND City of Portland, Bureau of Purchases, Contract Compliance Specialist, 112 SW 5<sup>th</sup> Avenue, Room 750, Portland, OR 97204

INSTRUCTIONS FOR COMPLETING THE MONTHLY SUBCONSULTANT PAYMENT AND UTILIZATION REPORT

EXHIBIT A

1. **SOLICITATION NUMBER:** Enter City of Portland solicitation number.
2. **CONTRACT NUMBER:** Indicates the contract number assigned by the City Auditor for this project.
3. **PRIME CONSULTANT:** Indicate the name of the prime consultant.
4. **PRIME CONTRACT AMOUNT:** Indicate the total dollar amount of the prime contract.
5. **REPORT DATES:** Indicate the beginning and ending dates corresponding to the progress payment period or use calendar month (i.e. 1/1/02 thru 1/31/02); reports should be sequential and not overlap.
6. **PROJECT NAME:** Indicate the project name as indicated on the contract documents.
7. **PROGRESS REPORT NUMBER:** Enter report No.1 for the first report submitted and sequential numbers for reports submitted thereafter.
8. **ALL SUBCONSULTANT NAMES:** List the names of all subconsultants listed on the original First-Tier Subconsultant Disclosure form as submitted at solicitation due date.
9. **ORIGINAL SUBCONTRACT AMOUNT:** Indicate the dollar amount for each subconsultant at time of award.
10. **AMENDED SUBCONSULTANT AMOUNT:** This amount should be the total dollar value (original subconsultant amount plus any additions or deletions) of the subcontract.
11. **PAYMENT AMOUNTS AND DATES MADE, FOR MONTH:** Please list any payment amounts for the month, and the dates the payments were made.
12. **TOTAL PAYMENTS, TO DATE:** This amount should be the total dollar amount paid-to-date to the subconsultant.

*SUBCONSULTANTS ADDED AFTER PROJECT WAS AWARDED*

13. **SUBCONSULTANT NAME:** Please list any subconsultants not appearing on original disclosure form.
14. **NATURE OF WORK:** Briefly describe subconsultants work (i.e. CAD drafting, environmental testing, etc.).
15. **STATUS:** Indicate the appropriate MW/ESB status of each subconsultant listed (i.e. MBE, WBE, ESB). **Note:** Designations should be consistent with how firms were certified by the State at time of contract award. Leave blank for non-certified firms.
16. **SUBCONSULTANT AMOUNT:** Indicate the dollar amount of the subcontract.
17. **PAYMENT AMOUNTS AND DATES MADE, FOR MONTH:** Please list any payment amounts for the month, and the dates the payments were made.
18. **TOTAL PAYMENTS, TO DATE:** This amount should be the total dollar amount paid-to-date to the subconsultant

COMMENTS (Include why any payment amounts made to a subconsultant are less than that requested by the subconsultant).

---

---

---

EXHIBIT A

EXHIBIT B

INDEPENDENT CONTRACTOR CERTIFICATION STATEMENT

SECTION A

CONTRACTOR CERTIFICATION I, undersigned, am authorized to act on behalf of entity designated below, hereby certify that entity has current Workers' Compensation Insurance.

Contractor Signature Ala Fygon Date 4/21/08 Entity Coalfire

If entity does not have Workers' Compensation Insurance, City Project Manager and Contractor complete remainder of this form.

SECTION B

ORS 670.600 Independent contractor standards. As used in various provisions of ORS Chapters 316, 656, 657, and 701, an individual or business entity that performs labor or services for remuneration shall be considered to perform the labor or services as an "independent contractor" if the standards of this section are met. The contracted work meets the following standards:

- 1. The individual or business entity providing the labor or services is free from direction and control over the means and manner of providing the labor or services, subject only to the right of the person for whom the labor or services are provided to specify the desired results;
2. The individual or business entity providing labor or services is responsible for obtaining all assumed business registrations or professional occupation licenses required by state law or local government ordinances for the individual or business entity to conduct the business;
3. The individual or business entity providing labor or services furnishes the tools or equipment necessary for performance of the contracted labor or services;
4. The individual or business entity providing labor or services has the authority to hire and fire employees to perform the labor or services;
5. Payment for the labor or services is made upon completion of the performance of specific portions of the project or is made on the basis of an annual or periodic retainer.

City Project Manager Signature \_\_\_\_\_ Date \_\_\_\_\_

SECTION C

Independent contractor certifies he/she meets the following standards:

- 1. The individual or business entity providing labor or services is registered under ORS Chapter 701, if the individual or business entity provides labor or services for which such registration is required;
2. Federal and state income tax returns in the name of the business or a business Schedule C or form Schedule F as part of the personal income tax return were filed for the previous year if the individual or business entity performed labor or services as an independent contractor in the previous year; and
3. The individual or business entity represents to the public that the labor or services are to be provided by an independently established business. Except when an individual or business entity files a Schedule F as part of the personal income tax returns and the individual or business entity performs farm labor or services that are reportable on Schedule C, an individual or business entity is considered to be engaged in an independently established business when four or more of the following circumstances exist. Contractor check four or more of the following:

- A. The labor or services are primarily carried out at a location that is separate from the residence of an individual who performs the labor or services, or are primarily carried out in a specific portion of the residence, which portion is set aside as the location of the business;
B. Commercial advertising or business cards as is customary in operating similar businesses are purchased for the business, or the individual or business entity has a trade association membership;
C. Telephone listing and service are used for the business that is separate from the personal residence listing and service used by an individual who performs the labor or services;
D. Labor or services are performed only pursuant to written contracts;
E. Labor or services are performed for two or more different persons within a period of one year; or
F. The individual or business entity assumes financial responsibility for defective workmanship or for service not provided as evidenced by the ownership of performance bonds, warranties, errors and omission insurance or liability insurance relating to the labor or services to be provided.

Contractor Signature \_\_\_\_\_ Date \_\_\_\_\_

# EXHIBIT A

## EXHIBIT C

### INSURANCE (The Project Manager must answer and initial 2, 3, and 4 below)

During the term of this contract Contractor shall maintain in force at its own expense, each insurance noted below:

1. Workers' Compensation insurance in compliance with ORS 656.017, which requires subject employers to provide Oregon workers' compensation coverage for all their subject workers (contractors with one or more employees, unless exempt under ORS 656.027).

- 
2.  Required and attached or Waived by City Attorney : \_\_\_\_\_

General Liability insurance with a combined single limit of not less than \$1,000,000 per occurrence for Bodily Injury and Property Damage. It shall include contractual liability coverage for the indemnity provided under this contract, and shall provide that City of Portland, and its agents, officers, and employees are Additional Insured but only with respect to the Contractor's services to be provided under this Contract:

3.  Required and attached or Waived by City Attorney : \_\_\_\_\_

Automobile Liability insurance with a combined single limit of not less than \$1,000,000 per occurrence for Bodily Injury and Property Damage, including coverage for owned, hired, or nonowned vehicles, as applicable:

4.  Required and attached or Waived by City Attorney : \_\_\_\_\_

Professional Liability insurance with a combined single limit of not less than \$1,000,000 per claim, incident, or occurrence. This is to cover damages caused by error, omission or negligent acts related to the professional services to be provided under this contract. If insurance coverage is provided on a "claims made" basis, the successful Proposer shall acquire a "tail" coverage or continue the same coverage for three years after completion of the contract, provided coverage is available and economically feasible. If such coverage is not available or economically feasible, contractor shall notify City immediately.

5. On all types of insurance. There shall be no cancellation, material change, reduction of limits, or intent not to renew the insurance coverage(s) without 30-days written notice from the Contractor or its insurer(s) to the City.

6. Certificates of insurance. As evidence of the insurance coverages required by this contract, the Contractor shall furnish acceptable insurance certificates to the City at the time contractor returns signed contracts. The certificate will specify all of the parties who are Additional Insured and will include the 30-day cancellation clause that provides that the insurance shall not terminate or be cancelled without 30 days written notice first being given to the City Auditor. Insuring companies or entities are subject to City acceptance. If requested, complete policy copies shall be provided to the City. The Contractor shall be financially responsible for all pertinent deductibles, self-insured retentions, and/or self-insurance.