

**AGREEMENT BETWEEN THE CITY OF SAN JOSÉ
AND
SCHEIDT & BACHMANN USA, INC.
FOR AN UPGRADE AND EXPANSION
TO A PARKING REVENUE CONTROL SYSTEM**

This Agreement is entered into as of February ____, 2009 between the City of San José, a municipal corporation ("City"), and Scheidt & Bachmann USA, Inc. a Delaware corporation ("Contractor").

RECITALS

1. On December 16, 2003 City and Contractor entered into a contract for the purchase and installation of Downtown Parking and Revenue Control System (PARCS)
2. Through subsequent amendments to the Agreement, the System was expanded to other downtown parking facilities;
3. City now desires to have Contractor install an software Upgrade in order to bring the System into compliance with current credit card payment security practices
4. City additionally desires to expand the upgraded System to its parking facility located at Second and San Carlos in San Jose.

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1 AGREEMENT DOCUMENTS

The documents forming the entire Agreement between City and Contractor shall consist of this Agreement including:

- EXHIBIT A - Scope of Services
 - EXHIBIT A-1 – Technical and Security Requirements
 - EXHIBIT A-2 – PCI Responsibility Matrix
- EXHIBIT B - Compensation
 - EXHIBIT B-1, Master Price List
- EXHIBIT C - Insurance Requirements
- EXHIBIT D – Software License Agreement
- EXHIBIT E - Change Order Form
- EXHIBIT F – Labor Compliance Addendum
- EXHIBIT G – Project Plan

In the event any discrepancies or inconsistencies between the provisions of this Agreement and any of the above-referenced documents arise, the provisions of this Agreement will prevail. Notwithstanding the foregoing, the term of the License Agreement and the Maintenance Agreement shall be as provided in the respective agreements.

This Agreement and the Exhibits set forth above, contain all of the agreements, representations and understandings of the Parties hereto, and supersede and replace any previous understandings, commitments, or agreements, whether oral or written. Any other terms or conditions included in any shrink-wrap or boot-screen license agreements, quotes, invoices, acknowledgments, bills of lading, or other forms utilized or exchanged by the Parties shall not be incorporated in this Agreement or be binding upon the Parties unless the Parties expressly agree in writing or unless otherwise provided for in this Agreement.

2 TERM OF AGREEMENT

The term of this Agreement is from February 3, 2009 to August 30, 2010, inclusive, subject to the provisions of Section 11. Notwithstanding the foregoing, the term of the License Agreement and the Maintenance Agreement shall be as provided in the respective agreements.

3 SCOPE OF SERVICES

3.1 Scope of Work

Contractor agrees to perform the services set forth in the Scope of Services which is attached as Exhibit A hereto and incorporated as though fully set forth herein (the "SOS").

3.2 Equipment

Any additional equipment required for final system acceptance as detailed in Scope of Services (Exhibit A) but not reflected in the Contractor's proposal and pricing shall be the sole responsibility of the Contractor and at no cost to the City. City reserves the right to purchase equipment separately if it receives more favorable pricing from third party, and the equipment corresponding price shall be deducted from Contractor's overall price.

3.3 Notification

Contractor agrees to notify City promptly of any factor, occurrence, or event coming to its attention that may affect Contractor's ability to meet the requirements of the Agreement, or that is likely to occasion any material delay in completion of the projects contemplated by this Agreement. Such notice shall be given in the event of any loss or reassignment of key employees, threat of strike, or major equipment failure.

3.4 Contractor's Software

The terms of the licensing of the Software is licensed to City and shall be as set forth in the Software License Agreement (Exhibit D).

3.5 Non- Contractor Software

Contractor shall procure, on City's behalf, the Third Party Software, pursuant to and in accordance with the license and maintenance agreements attached hereto as Exhibit D. City shall execute and deliver the license and maintenance agreements for the Third Party Software. City shall comply with the terms and conditions of such agreements, provided that Contractor may serve as City's agent for purposes of obtaining and implementing the items and services contemplated by such agreements. Contractor shall obtain from all suppliers of the equipment and the Third Party Software, all standard guarantees and warranties normally provided on all machinery, equipment, services, materials, supplies and other items used in connection with the performance of the Services, including all such machinery,

equipment, materials and other items which are incorporated into the System. Contractor shall obtain from each such supplier guarantees and warranties which are assignable to City and which cover the Warranty Period and shall, upon request of City, obtain an option for City to purchase a guarantee or warranty from such suppliers covering a longer period than the Warranty Period if commercially available at City's expense. Contractor shall enforce all guarantees and warranties until such time as such guarantees or warranties expire or are, if applicable, transferred to City as contemplated by this Section 3. Such guarantees and warranties shall, to the extent they have been made assignable, be transferred to City upon expiration or termination of this Agreement. Such guarantees and warranties shall, to the extent they have been extended, be transferred to City upon the earlier to occur of (1) the expiration of the Warranty Period, and (2) termination of this Agreement. Contractor shall, to the extent that a warranty or guaranty has been extended or made assignable to City pursuant to this Section 3, deliver to City copies of all such guarantees and warranties and relevant extracts from all related technical specifications. Nothing in this Section 3 shall derogate from the obligations of Contractor to provide the guarantees and warranties described in, and to comply with the provisions of this Agreement.

3.6 Maintenance Services

After the warranty period, the terms of maintenance of the System shall be as set forth in the Scope of Services.

4 STANDARDS OF SERVICE

In connection with the performance of any Services pursuant to this Agreement:

4.1 Number of employees

Contractor warrants it will provide sufficient employees to complete the Services ordered within the applicable time frames as presented in Exhibit G (Project Plan) to this Agreement. Furthermore, Contractor shall, at its expense, supply all tools, equipment and other materials necessary to perform the Services contemplated in this Agreement.

4.2 Skill of Employees

Contractor warrants that employees shall have sufficient skill, knowledge, and training to perform Services and that the Services shall be performed in a professional and workmanlike manner.

4.3 Duty of confidentiality

All data, documents, discussions or other information developed or received by or for one party in performance of this Agreement are confidential and must not be disclosed to any person except as authorized by the other party, or as required by law. The receiving party warrants that all employees utilized by it in performing Services are under a written obligation to the receiving party requiring the employee to maintain the confidentiality of information of the other party.

4.4 Security and Safety

Contractor shall require employees providing Services at a City location to comply with applicable City security and safety regulations and policies. City may require each employee providing Services to undergo a background investigation, including a criminal records and

fingerprint check. Contractor shall promptly replace any employee found to be unacceptable to City, in its discretion, on the basis of a significant infraction found in the background investigation.

4.5 Contractor's obligations to employees

Contractor shall provide for and pay the compensation of employees and shall pay all taxes, contributions, and benefits (such as, but not limited to, workers' compensation benefits) which an employer is required to pay relating to the employment of employees. City shall not be liable to Contractor or to any employee for Contractor's failure to perform its compensation, benefit, or tax obligations. Contractor shall indemnify, defend and hold City harmless from and against all such taxes, contributions and benefits and will comply with all associated governmental regulations, including the filing of all necessary reports and returns.

4.6 Replacement of employees

During the course of performance of Services, City may request replacement of an employee or a proposed employee, provided that there is reasonable cause. In such event, Contractor shall, within five (5) working days of receipt of such request from City, provide a substitute employee of sufficient skill, knowledge, and training to perform the applicable Services. If, within the first thirty (30) days after an employee's commencement of Services, City notifies Contractor (1) such employee's level of performance is unacceptable, (2) such employee has failed to perform as required, or (3) such employee, in City's sole opinion, lacks the skill, knowledge or training to perform at the required level, then Contractor will be required to review the work performed by said employee, confirm the quality of work, and correct any items the Contractor deems incorrect. If City requests replacement of an employee for the above-referenced reasons after such thirty (30) day time period, or at any time for a reason other than the reasons indicated above.

4.7 Schedule of Performance

Contractor shall perform the Services according to the terms and provisions of the Milestone Schedule contained in Exhibit G, Project Plan. Time is expressly made of the essence with respect to each and every term and provision of this Agreement.

5 CHANGE ORDER PROCEDURE AND AUTHORIZATION

5.1 Changes

Any changes to this Agreement after the Effective Date that relate to (i) the deletion of Products or Services, (ii) adding additional Products or Services, (iii) changing or modifying Products or Services, or (iv) making other changes that materially alter the scope of this Agreement or the Deliverables required under this Agreement, including approval of all performance and/or payment schedules shall be made by the Director of Finance in accordance with the procedures set forth below.

5.2 Contract Change Requests

Either party hereto may, from time to time, and at any time during the term hereof request a change, as defined in the above section. (The party requesting the change is hereinafter referred to as the "Requesting Party.") Requests for changes shall be in writing and shall be addressed and delivered to the other party. Such writing shall be identified as a "Contract Change Request," shall carry a sequential number for ease of tracking, shall set forth in

detail the nature of the change requested and the costs associated therewith, and shall identify the Products, Services, Deliverables or Schedules to be changed.

5.3 Procedures

As soon as practical after receipt by the notified party of copies of the Request, the parties shall as necessary meet to discuss the change and to ascertain its cost and schedule impacts, if any.

5.4 Change Orders

If the parties decide to implement a change request, a standard form Change Order ("CO") shall be prepared in a form substantially similar to the form attached hereto as Exhibit E, which CO shall describe the change, delineate the cost, schedule, and other impacts of the change and the payment terms for any price increase. Only City's Director of Finance and Contractor's Authorized Representative shall have authority to execute CO's to this Agreement. Execution of a CO by City's Director of Finance and Contractor's Authorized Representative shall constitute a modification hereof and shall be binding on both parties hereto.

6 COMPENSATION

6.1 Contract Price

The Total Contract Price in U.S. dollars shall not exceed Six Hundred Seventy Five Thousand, One Hundred Forty Eight Dollars and No Cents (U.S. \$675,148.00) ("Maximum Compensation"). The terms, rate and schedule of payment are set forth in the attached Exhibit B, entitled "Compensation." Contractor will submit to City invoices that include a breakdown of services provided for the corresponding milestone in accordance to attached Exhibit B, entitled "Compensation." City will make payments to Contractor within thirty (30) days after the date of each invoice. City will make payments when due in the form of a check, cashier's check, or wire transfer drawn on a U.S. financial institution.

6.2 Freight, Title, and Risk of Loss

All freight charges will be pre-paid by Contractor and added to the invoices. Title to the Equipment will pass to City upon delivery and full payment, except that title to Software will not pass to City at any time. Risk of loss will pass to City upon delivery of the Equipment to the City. Contractor will pack and ship all Equipment in accordance with good commercial practices.

7 TAXES AND CHARGES

Contractor shall be responsible for payment of all taxes, fees contributions or charges applicable to the conduct of Contractor's business.

8 LABOR COMPLIANCE

This Agreement is subject to City's Prevailing/Living Wage Policy and the applicable implementing regulations (collectively, the "Policy"). Contractor shall comply with the provisions of the attached Labor Compliance Addendum (Exhibit F), which sets forth Contractor's obligations under the Policy.

9 SYSTEM ACCEPTANCE(ONLY APPLICABLE TO 2ND/SAN CARLOS)

Upon completion of final installation, City and Contractor shall conduct an Acceptance Test upon the System. The criteria for the Acceptance Test shall be as set forth in the Scope of Work (Exhibit A). System Acceptance will occur upon successful completion of the Acceptance Tests described in the Acceptance Test Plan. When System Acceptance occurs, the parties will memorialize this event by promptly executing a System Acceptance Certificate.

If, in the discretion of City, the System does not meet the requirements of the Acceptance Test specifications as described in the Scope of Services, City requires Contractor to repair the System so that the same meets the Acceptance Test specifications in all material respects, all at no additional expense to City. All warranties shall become effective and begin to run as presented in Exhibit A, Scope of Services, and Exhibit D, Software License, of this agreement.

City will give Contractor written notice of successful completion of any testing program within fifteen (15) business days after end of each testing. If City fails to issue any letter of notice within this period the date of the according completion shall be deemed as day of acceptance of the tested portion of work. Final acceptance will be deemed according to the same criteria, if no major malfunctions were indicated by City or its representatives during the Acceptance Test, which prevent putting the system into operation for customer services.

Payment for any part or parts of the System or Services provided hereunder, or inspection or testing thereof by City, shall not constitute acceptance or relieve Contractor of its obligations under this Agreement. City may inspect the components of the System when delivered and reject upon notification to Contractor any and all the System which does not conform to the Specifications or other requirements of this Agreement. Components of the System which are rejected shall be promptly corrected, repaired, or replaced by Contractor in accordance with Contractor's warranty obligations under this Agreement, such that the System conforms to the warranties, Specifications and the other requirements of this Agreement. If City receives components of the System with defects or nonconformities not reasonably apparent on inspection, then City reserves the right to require prompt correction, repair, or replacement by Contractor in accordance with Contractor's warranty obligations under this Agreement following the discovery of such defect or nonconformity.

10 REPRESENTATIONS

10.1 Prime Contractor Responsibility

Contractor understands and accepts full responsibility as the Prime Contractor for all requirements and deliverables defined in this Agreement. Contractor warrants it:

1. Has read and agrees with the specifications contained in the Scope of Services (Exhibit A);
2. Fully understands the facilities, difficulties, and restrictions attending performance of the services; and
3. Contractor also agrees to inform City of any known conditions prior to the execution of this Agreement which will materially affect performance of the work within 45 days of

the execution of this Agreement and shall not proceed until written instructions are received from City Any conditions which become known after execution of this Agreement must be communicated to City within five (5) days of occurrence and shall not proceed until written instructions are received from the City.

10.2 Missing and Incompatible Hardware Components.

Contractor understands that City has relied upon the expertise of Contractor in the determination of all Parking Access and Revenue Control System hardware components to effectively address the specifications and requirements of this Agreement. As such, Contractor assumes full responsibility and financial risk to insure that all required hardware components are included in the System design described in the Scope of Services.

1. In the event that any hardware component required to operate or maintain the System in accordance with the performance requirements, as detailed in the Scope of Services contained in this Agreement is missing; or
2. Any Contractor-supplied or specified hardware component is proven to be incompatible with the System design, such proof being evidenced by elimination of any error by the removal or replacement of the offending hardware component, Contractor shall provide the missing or replace the incompatible hardware component at no additional charge to City. Contractor's actions to remedy the situation shall be in accordance with the error levels defined in the Warranty and Maintenance Agreement under the Duties Section. (Exhibit D).

10.3 Authority to Make Agreement.

Contractor represents and warrants that Contractor has full right and authority to perform its obligations under this Agreement. City shall be entitled to use the System without disturbance.

10.4 Contractor Agreements with City Employees.

Neither Contractor nor any director, employee or agent of Contractor or its subcontractors or vendors shall knowingly, without prior written notification thereof to City, enter into any business relationship with any employee or agent of City unless such person is acting for and on behalf of City.

11 TERMINATION

11.1 Termination for Convenience

City shall have the right to terminate this Agreement, without cause, by giving not less than sixty (60) days' written notice of termination.

11.2 Termination for Default

If Contractor fails to perform any of its material obligations under this Agreement, in addition to all other remedies provided by law, City will issue a notice to cure. Contractor will satisfactorily respond to the notice to cure within 15 business days of issuance. If the Contractor does not satisfactorily respond to the notice to cure within 15 days or consistently and repetitively fails to cure, City may terminate this contract immediately upon written notice.

11.3 Termination Authority

The Director of Finance ("Director") is empowered to terminate this Agreement on behalf of City.

11.4 Consequences of Termination

In the event of termination, Contractor shall deliver to City copies of all reports, documents, and other work performed by Contractor under this Agreement, and upon receipt thereof, City shall pay Contractor for services performed and reimbursable expenses incurred to the date of termination.

12 INDEMNIFICATION

Contractor shall defend, indemnify and hold harmless City, its officers, employees and agents against any claim, loss or liability arising out of or resulting in any way from work performed under this Agreement due to the willful or negligent acts (active or passive) or omissions by Contractor's officers, employees or agents. The acceptance of said services and duties by City shall not operate as a waiver of such right of indemnification.

13 LIABILITY FOR DAMAGES

Contractor maintains insurance with coverage for the US, according to Section 16, Insurance Requirements and Exhibit C, including but not limited to General Liability and Product Liability Insurance with a total value of coverage above 25 million (€25,000,000) euros. Any damages the City may claim are in any case restricted to payments available under this insurance. The aggregate liability of Contractor on all claims of any kind by the City of San Jose shall in no event exceed the maximum possible insurance coverage, which in no event shall be less than 25 million (€25,000,000) euros.

14 OWNERSHIP AND CONTROL OF THE DATA

The City shall maintain ownership and control of the data throughout the Agreement period. Contractor shall have the right to use the data solely to perform services under the Agreement with the City. Contractor may not use the data, a subset of the data, and/or a summary of the data, or, cause or permit the data, a subset and/or a summary, to be used by any third party, outside the scope of the Agreement without the express written consent of the City. Contractor shall provide City with a copy of the data in a mutually agreed upon format at regular intervals and at such additional times as the City deems appropriate. Contractor warrants that throughout all operational and maintenance activities the accuracy of the database will be preserved.

15 INSURANCE REQUIREMENTS

Contractor agrees to have and maintain the policies set forth in Exhibit C, entitled "Insurance Requirements," which is attached hereto and incorporated herein. All policies, endorsements, certificates and/or binders shall be subject to approval by the Risk Manager of the City of San Jose as to form and content. These requirements are subject to amendment or waiver if so approved in writing by the Risk Manager. Contractor agrees to provide City with a copy of said policies, certificates and/or endorsements before work commences under this Agreement.

16 WAIVER

Contractor agrees that City's waiver of any breach or violation of any provision of this Agreement shall not be deemed to be a waiver of any other provision or a waiver of any subsequent breach or violation of the same or any other provision. City's acceptance of the performance of any of Contractor's services will not be a waiver of any provision of this Agreement.

17 INDEPENDENT CONTRACTOR

Contractor, in the performance of this Agreement, is an independent contractor. Contractor shall maintain complete control over all of Contractor's employees, any subcontracting subcontractors, and Contractor's operations. Neither Contractor nor any person retained by Contractor may represent, act, or purport to act as the agent, representative or employee of City. Neither Contractor nor City is granted any right or authority to assume or create any obligation on behalf of the other.

18 COMPLIANCE WITH LAWS

Contractor shall comply with all applicable laws, ordinances, codes and regulations (collectively, "laws") of the federal, state and local governments, including without limitation, any and all laws specified elsewhere in this Agreement.

19 CONFLICT OF INTEREST

Contractor shall avoid all conflict of interest or the appearance of conflict of interest in performance of this Agreement.

20 NONDISCRIMINATION

Contractor agrees that there shall be no discrimination against, or segregation of, any person, on account of race, sex, color, age, religion, sexual orientation, actual or perceived gender identity, disability, ethnicity, national origin, marital status, or family status, in connection with or related to the performance of this Agreement.

21 GIFTS

21.1 Prohibition on Gifts

Contractor acknowledges that Chapter 12.08 of the San Jose Municipal Code prohibits City's officers and designated employees from accepting gifts as defined in Chapter 12.08.

21.2 No Offer

Contractor agrees not to offer any City officer or designated employee any gift prohibited by Chapter 12.08.

21.3 Breach of Agreement

Contractor's offer or giving of any gift prohibited by Chapter 12.08 will constitute a material breach of this Agreement. In addition to any other remedies City may have in law or equity,

City may terminate this Agreement for such breach as provided in Section 12 of this Agreement.

22 DISQUALIFICATION OF FORMER EMPLOYEES

Contractor is familiar with Chapter 12.10 of the San Jose Municipal Code ("Revolving Door Ordinance") relating to the disqualification of City's former officers and employees in matters which are connected with their former duties or official responsibilities. Contractor shall not utilize either directly or indirectly any officer, employee, or agent of Contractor to perform services under this Agreement, if in the performance of such services, the officer, employee, or agent would be in violation of the Revolving Door Ordinance.

23 CONTRACTOR'S BOOKS AND RECORDS

23.1 Maintenance during Term

Contractor shall maintain any and all ledgers, books of account, invoices, vouchers, canceled checks, and other documents evidencing or relating to charges for services, or expenditures and disbursements charged to City for a minimum period of three (3) years and maximum of seven (7) years from the date of final payment to Contractor pursuant to this Agreement.

23.2 Maintenance after Term

Contractor shall maintain all documents, which demonstrate performance under this Agreement for a minimum period of three (3) years and maximum of seven(7) years, from the date of termination or completion of this Agreement.

23.3 Inspection

Any documents required to be maintained pursuant to this Agreement must be made available for inspection or audit, at any time during regular business hours, upon written request by the City Attorney, City Auditor, City Manager, or a designated representative of any of these officers. Contractor shall provide copies of such documents to City for inspection at City Hall when it is practical to do so. Otherwise, unless an alternative is mutually agreed upon, the records shall be available at Contractor's address indicated for receipt of notices in this Agreement.

24 ASSIGNABILITY

The parties agree that the expertise and experience of Contractor are material considerations for this Agreement. Unless specifically authorized by this Agreement, Contractor may not assign the performance of any obligation or interest under this Agreement without the prior written consent of City. Any attempt by Contractor to assign this Agreement, in violation of this Section, will be voidable at City's sole option.

25 SUBCONTRACTORS

25.1 Authorized Subcontractors

Notwithstanding Section 24 (Assignability) above, Contractor may use designated subcontractors at its own discretion.. Contractor shall be responsible for directing the

work of the approved subcontractors and for any compensation due to subcontractors. City assumes no responsibility whatsoever concerning such compensation.

25.2 Compliance with Agreement

Contractor shall ensure that Contractor's subcontractors comply with this Agreement. At City's request, Contractor shall require any or all of Contractor's subcontractors to sign an agreement with Contractor requiring compliance with this Agreement.

26 GOVERNING LAW

This Agreement must be construed -- and its performance enforced--under California law.

27 VENUE

In the event that suit is brought by either party to this Agreement, the parties agree that venue must be exclusively vested in the state courts of the County of Santa Clara, or where otherwise appropriate, exclusively in the United States District Court, Northern District of California, San Jose, California.

Contractor further agrees that in the event a lawsuit involving this Agreement is filed by City, Contractor will unconditionally accept the jurisdiction of a federal or state court located in Santa Clara County, California.

28 NOTICES

All notices and other communications required or permitted to be given under this Agreement must be in writing and must be personally served, or mailed, postage prepaid via U. S. mail, or sent via courier service, addressed to the respective parties as follows:

To City: Director of Finance
 City of San Jose
 200 East Santa Clara Street
 San Jose, CA 95113

To Contractor: Vice President, Administration
 Scheidt & Bachmann USA Inc.
 31 North Avenue
 Burlington MA 01803

Notice will be effective on the date personally delivered or if sent by courier service, on the date of receipt. If mailed, notice will be effective three (3) days after deposit in the mail.

The parties may change their respective addresses in accordance with the provisions of this Section.

29 MISCELLANEOUS

29.1 Survival of Provisions

If any part of this Agreement is for any reason found to be unenforceable, all other parts nevertheless remain enforceable.

29.2 Assignment

Subject to the provisions of Section 24 (Assignability), this Agreement binds and inures to the benefit of the parties and their respective successors and assigns.

29.3 Headings

The headings of the sections and exhibits of this Agreement are inserted for convenience only. They do not constitute part of this Agreement and are not to be used in its construction.

29.4 Authority of City Manager

Where this Agreement requires or permits City to act and no officer of the City is specified, City's Manager or the designated representative of City's Manager has the authority to act on City's behalf.

APPROVED AS TO FORM:

City of San José
a municipal corporation

Senior Deputy City Attorney

By _____
Name:
Title:
Date: _____

Scheidt & Bachmann USA, Inc.
a Delaware Corporation


By _____
Name: John C. MacDonnell
Title: Treasurer
Date: 1/21/2009

EXHIBIT A

SCOPE OF SERVICES

1 PROJECT OVERVIEW

1.1 The City of San Jose (City) has previously contracted with Scheidt & Bachmann (Contractor) for the installation of Contractor's PARCS at the Market/San Pedro, 3rd Street, Convention Center, 4th/San Fernando, City Hall, and 4th/St. John (Civic Center) Garages shall provide a complete and operating PARCS and PCI / EnterVo System upgrade for PCI/PABP compliance (Upgrade). All labor, plans, installation, materials, tools, equipment, transportation, hauling and stockpiling, and incidentals, required to fulfill the above shall be furnished and installed whether or not specifically enumerated herein. The Upgrade installation will be handled as a "turnkey project".

1.2 City will be replacing their existing Parking Access and Revenue Control System, PARCS, at the 2nd/San Carlos Garage with a new system and upgrading the City's existing This work will include system design, configuration, removal of existing equipment at 2nd/San Carlos, and installation of hardware components and software, testing as set forth in this document. The City will provide, under a separate DOT project the necessary electrical and communication conduits, modify entrance and exit islands, and install protective bollards.

2 SPECIFICATIONS FOR PCI UPGRADE PROJECT

2.1 Contractor will upgrade the City's PARCS enterVo system with a credit card processing module compliant as mandated by the Visa Payment Application Best Practices (PABP) and install a PA-DSS compliant version within the timeline established by the PCI Data Security Standard Council (Council). The current target date is April 2009. The Contractor and City understand that the Council may change this compliance date; and that Contractor will meet the new target date to maintain PA-DSS compliance. The enterVo application software credit card module is technically compliant and meets or exceeds the requirements listed in the PABP standards.

2.2 The PABP is a set of requirements that the POS application developer follows to maintain a high level of security within their applications. S&B ensures that the PARCS application provided meets the card associations' application best practice standards, including Visa USA's PABP standards as it relates exclusively to the application software:

2.2.1 Does not retain full magnetic stripe

2.2.2 Protects stored data

2.2.3 Provides secure password features

2.2.4 Logs application activity

2.2.5 Develops secure applications

2.2.6 Tests applications to address vulnerabilities

2.2.6.1 Facilitates secure remote software updates

2.2.6.2 Facilitates secure remote access to application

2.2.6.3 Restricts internal administrative access

2.2.7 Overall Approach

The S&B enterVo PARCS consists of software and some hardware upgrades to entry, exit, pay machine, facility and central system computers and servers controlling the overall operation. The primary elements of the project are:

- 2.2.7.1** System design services including, but not limited to, full review of current operational practices, review of current PARCS reporting module, review enterVo reporting module, provide operation comparison matrix indicating current and new system modules, enterVo configuration, and System design documentation
- 2.2.7.2** Provide Server and additional computer equipment and necessary associated software configuration as identified in Exhibit B-1, Master Price List.
- 2.2.7.3** Provide field equipment software upgrade to enterVo using existing and new hardware as identified in Exhibit B-1, Master Price List.
- 2.2.7.4** Additional services and software licenses as identified in Exhibit B-1, Master Price List.

2.2.8 Scheidt & Bachmann will install the PARCS enterVo 30/PCI upgrades at the following locations:

- 2.2.8.1** Convention Center
- 2.2.8.2** Market/San Pedro
- 2.2.8.3** 3rd Street
- 2.2.8.4** 4th/San Fernando
- 2.2.8.5** City Hall
- 2.2.8.6** Civic Center (4th/St. John)
- 2.2.8.7** 3rd/Santa Clara (Globe)
- 2.2.8.8** 2nd/San Carlos

2.2.9 The CreditPay module provided with the ICverify interface is technically compliant and meets or exceeds the requirements listed in the PABP standards. The interface will be provided for the City’s designated clearing house First Data Merchant Services.

2.3 SUBMITTALS

The following documents will be delivered as identified:

	Description	Due
1	Project Schedule including all activities of subcontractor and others; and PCI Data Security Standard Security Audit Procedures Version 1.2 Responsibility Matrix.	30 days from approval of agreement by City Council
2	System Design Document that clearly defines the system configuration and deliverables	90 days prior to installation
3	Acceptance Test Document	30 days prior to Testing
4	Training schedule and syllabus	30 days prior to Training
5	PARCS/enterVo Documentation including manuals for cashier, supervisor, system	30 days prior to training

	Description	Due
	administrator and maintenance	
6	System/Network Diagram including IP addresses, device and lane names and all network devices including type, model number and physical location	Prior to start of 30 day acceptance test

2.3.1 System Design Document

2.3.1.1 The system design services will include meetings with City staff and development of a design document including configuration of enterVo application software, modules, reports, rate programming, authorized users, devices, lanes and facilities and all other elements necessary to properly configure and program the enterVo system for the City by Contractor.

2.3.1.2 The final result of the 'System Design Services' is the creation of a System Design Document (SDD) that clearly defines the system configuration and deliverable. It is expected that the City will be heavily involved in the creation of the SDD document in order to eliminate, as much as possible, the repetitive review process.

2.3.1.3 The City will be allowed 30 days from time of acceptance to deliver a list of report customization requests to the Contractor. Contractor will assign expected hours to each item on the list. Contractor and City will meet to determine prioritization of customization, task assignment and discuss change orders for those items deemed to exceed the report customization allowance of 20 hours. Contractor will include its standard report package with the new software. Additional report creation or customization will be addressed on a per request basis and may be subject to additional fees for development and deployment.

2.3.2 System/Network Drawing. Contractor will complete the system/network drawing and will include IP addresses, device and lane names and show all network devices including type, model number and physical location.

2.4 OPERATIONAL DESCRIPTION FOR ENTERVO

2.4.1 General

System requirements will be as described in the System Design Document and programming will be complete by the date of the Off-site Testing. At a minimum System requirements will be as set forth in Exhibit A, Scope of Services

2.4.2 Reports

The System will provide the enterVo Standard Report package, as described in the system manual required in Section 3.2.6, Item 3, that will reside on the Central Database Server. The report package will be accessible via browser from workstations on the parking network to those users with appropriate access rights.

2.4.3 Training

By means of training classes, Contractor shall provide System Administrator Level instruction in the operation, maintenance and administration of the PARCS including Credit Card Server and Rate Programming. Contractor will set up a facility controller

with enterVo software prior to the completed installation in San Jose. Training will be conducted in six (6) four (4) hour classes. Contractor will provide all training manuals. The City will provide an appropriate training room.

2.5 TEST CRITERIA

2.5.1 The Contractor shall notify the City of the time, date and place of all tests at least fourteen (14) calendar days prior to the date on which the on site tests are planned, except for the Off-site Test, which the City will not be present to witness. If requested by the City, the Contractor shall postpone the on-site test up to seven (7) calendar days in order to accommodate the schedule of the City and its representatives.

2.5.2 The City may waive the right to witness certain tests. Neither the witnessing of tests by the City, nor the waiving of the right to do so, will relieve the Contractor of the responsibility to furnish and install the work in accordance with the requirements of this RFP. City approval of any test results will not be deemed as acceptance of the equipment or systems tested until successful completion of the System Acceptance Test.

2.5.3 The Contractor shall provide confirmation to the City that all equipment and programming to be tested is ready for testing prior to the performance of the testing, and City's witnessing of the tests.

2.5.4 All test data forms shall be signed by the Contractor or authorized representative. The City or City's representative witnessing the testing shall also sign all test data forms and denote whether or not each test has successfully passed.

2.5.5 The contract period will not be extended for time loss or delays related to testing.

2.5.6 The Contractor shall conduct the following tests

2.5.6.1 PCI / enterVo Upgrade Project Off-site Test

2.5.6.2 On-site Installation Test

2.5.6.3 Acceptance Test

2.6 OFF-SITE TEST (PCI/ ENTERVO UPGRADE PROJECT)

2.6.1 Prior to delivery and installation of the PCI / enterVo Upgrades to San Jose, the Contractor will conduct an Off-site Test to provide verification of all site-specific programming features and functions that have been set forth in the System Design Document.

2.6.2 The Contractor will provide a written test document for the City's review at least thirty (30) days prior to the scheduled test. The City will not be present to witness the off-site test and will require written documentation from the Contractor to support the testing performed.

2.6.3 Testing will occur for a period sufficient to verify all site-specific features and functions that have been set forth in the System Design Document. All system deficiencies and discrepancies during the offsite test shall be corrected, resubmitted, and retested before the off-site test is complete.

2.7 ON-SITE INSTALLATION TESTS

2.7.1 After installation of PARCS or PCI/enterVo equipment and/or software at a Parking Facility, the Contractor will conduct an Installation Test in the presence of the City to provide verification of all site-specific features and functions that have been set forth in this scope of work. The test will include verification of all programming features and functions as specified in the scope of work.

2.7.2 The Contractor will provide a written test document for the City's review at least thirty (30) days prior to the scheduled test. The City and Contractor will witness the Installation test and will provide written documentation to support the testing performed.

2.7.3 Testing will occur for a period sufficient to verify all site-specific features and functions that have been set forth in this SOW. In the event of a failure during the installation test, the City shall notify the Contractor in writing of the failure. The Contractor shall replace or repair the equipment and a retest of the equipment will be required.

2.7.4 All system deficiencies and discrepancies during the installation test shall be corrected, resubmitted, and retested before the installation test is complete.

2.8 ACCEPTANCE TESTS (AT):

2.8.1 The City will verify that the PARCS, as installed, meets all functional requirements within this scope of work, including verification that the PARCS performs correctly with the CC.

2.8.2 The AT will occur after the successful completion of the Installation Test. The AT will run for a continuous thirty (30) day period unless the enterVo software fails to meet the standards for performance set forth in this scope of work.

2.8.3 In the event that the enterVo software fails the AT, the Contractor will have fourteen (14) calendar days to correct the problem. Once the Contractor has indicated in writing that the problems have been corrected, the test will resume from the date of the failure.

2.8.4 The City will provide the Contractor with written confirmation within fifteen business days upon the enterVo software passing the AT. In the event of a failure during the AT, the Contractor will correct the deficiency to the City's satisfaction and the Parking Manager will resume the test.

2.8.5 Any hardware failures that occur on equipment not replaced as a part of this system upgrade will not be considered a malfunction and will not impact the acceptance test.

2.9 WARRANTY

2.9.1 Equipment Warranty. Contractor warrants that equipment under normal use and service will be free from defects in material and workmanship for the applicable warranty period. The warranty period shall be one (1) year from the date of Beneficial Use. If City claims that equipment is non-conforming, City shall (1) promptly notify Contractor in writing of the basis of such nonconformity; (2) follow Contractor's instructions for return of the equipment; and (3) return the equipment freight prepaid to Contractor's designated location. Contractor shall at its own expense, repair or replace all the defective.

2.9.2 Software Warranties. Software Warranties shall be as set forth in the Software License (Exhibit D).

2.9.3 Software updates released to remedy or prevent software failures are included in the preventive maintenance scope of work. Software upgrades or updates which add new functionalities or where new functionalities require new or additional hardware shall not be included in the scope of preventive maintenance and Warranty

2.9.4 PCI Compliance Warranty. As part of the first year warranty, Contractor will perform regular required assessments and audits to maintain compliance with current and future credit card payment and security requirements. At the end of the warranty period, the City will have an option to enter a Credit Card Security Compliance Maintenance Agreement with Scheidt and Bachmann.

2.9.5 Before the expiration of the warranty period, City must notify Contractor in writing if Equipment or Contractor Software does not conform to these warranties. Upon receipt of such notice, Contractor will investigate the warranty claim. If this investigation confirms a valid warranty claim, Contractor will (at its option and at no additional charge to City) repair the defective Equipment or Contractor Software, replace it with the same or equivalent product, or refund the price of the defective Equipment or Contractor Software. Such action will be the full extent of Contractor's liability hereunder. Repaired or replaced product is warranted for the balance of the original applicable warranty period. All replaced products or parts will become the property of Contractor

3 SPECIFICATIONS FOR 2ND/SAN CARLOS GARAGE

3.1 FACILITY LOCATION:

280 S. 2nd Street
San Jose, CA 95113

3.2 SUMMARY OF DELIVERABLES

3.2.1 Parking Office

3.2.1.1 Install Facility Controller POS30/S including SL20 in Parking Office.

3.2.1.2 Install and set up Cisco security appliance for VPN access.

3.2.1.3 T1 Line and Router provided by City.

3.2.1.4 Install Intercom Controller in Network Rack provided by S&B

3.2.1.5 Install Network Switch in Network Rack provided by S&B

3.2.1.6 Install Intercom Master Station

3.2.2 Entry Lane

3.2.2.1 Install all Lane equipment supplied by S&B consisting of two (2) Ticket Dispensers, Barrier Gates, UPS-Systems according to S&B supplied Lane Layout drawings.

3.2.2.2 2 Loop configuration to allow motorcycle entry. Due to the design and material of motorcycles, Contractor cannot guarantee an accurate count via the two loop system for all entries.

3.2.2.3 Supply, pull and hook-up 22AWG, 10 conductors stranded, individually colored between Ticket Dispenser and Barrier Gate. Belden 5508UE or similar for Gate communication.

3.2.2.4 Supply, pull and hook up 12AWG Power cable from UPS to Ticket Dispenser and from Ticket Dispenser to Barrier Gate according to S&B Hookup drawings.

3.2.2.5 Supply, pull and hookup 14AWG Power cable from Ticket Dispenser to existing Lane Status Light (where available) according to S&B Hookup drawings.

3.2.2.6 Pre-pay functionality at the Entry device

3.2.3 Exit Lane

3.2.3.1 Install all Lane equipment supplied by S&B consisting of three (3) Exit Verifiers, Barrier Gates, UPS-Systems according to S&B supplied Lane Layout drawings.

3.2.3.2 2 Loop configuration to allow motorcycle exit. Due to the design and material of motorcycles, Contractor cannot guarantee an accurate count via the two loop system for all entries.

3.2.3.3 Supply, pull and hook-up 22AWG, 10 conductors stranded, individually colored between Ticket Dispenser and Barrier Gate. Belden 5508UE or similar for Gate communication.

3.2.3.4 Supply, pull and hook up 12AWG Power cable from UPS to Exit Verifier and from Exit Verifier to Barrier Gate according to S&B Hookup drawings.

3.2.3.5 Supply, pull and hookup 14AWG Power cable from Exit Verifier to existing Lane Status Light (where available) according to S&B Hookup drawings.

3.2.3.6 Supply, pull and hookup 14AWG Power cable from Exit Verifier to new Pedestrian Warning Devices.

3.2.4 Pay Machines

3.2.4.1 Install two (2) PKA30 supplied by S&B according to S&B installation drawings.

3.2.4.2 Install UPS System.

3.2.4.3 Hookup Power, provided by City to PKA30 according to S&B hookup drawings.

3.2.5 Network

3.2.5.1 Supply and pull 24AWG, 4 conductor TP from Control Lane 1, 2 (En), 3, 4 & 5 (Ex), and each PKA to Parking Office. Wire will be terminated and labeled in Parking Office inside S&B supplied Network Rack on punch-down Block.

3.2.5.2 Supply and pull CAT5 UTP from Control Lane 1, 2 (En), 3, 4 & 5 (Ex), and each PKA to Parking Office. Wire will be terminated and labeled in Parking Office inside S&B supplied Network Rack on punch-down block. Wire will be terminated in field Units with RJ45 Connector.

3.2.6 Submittals. The following documents will be delivered as identified:

Item	Description	Due
1	Project Schedule including all activities of subcontractor and others 2 nd & San Carlos	30 days from approval of agreement by City Council
2	Acceptance Test Document	30 days prior to Testing
3	PARCS Documentation including manuals for cashier, supervisor, system administrator and maintenance	30 days prior to training
4	System/Network Diagram including IP addresses, device and lane names and all network devices including type, model number and physical location	Prior to start of 30 day acceptance test
5	As Built Drawings	Prior to start of 30 day acceptance test

3.3 SYSTEM GEOMETRY

3.3.1 Network Media

Facilities	Lane Equipment	Switches to Parking Office (supplied and maintained by Contractor)	Parking Office to City Hall (supplied and maintained by City)
2 nd & San Carlos	100BaseT	100BaseFL	New T1 to be installed
Market Street Convention Center	100BaseT	100BaseFL	T1
3 rd Street City Hall 4 th & St. John	100BaseT	100BaseFL	Fiber
4 th & San Fernando	100BaseT	100BaseFL	New T1 to be installed

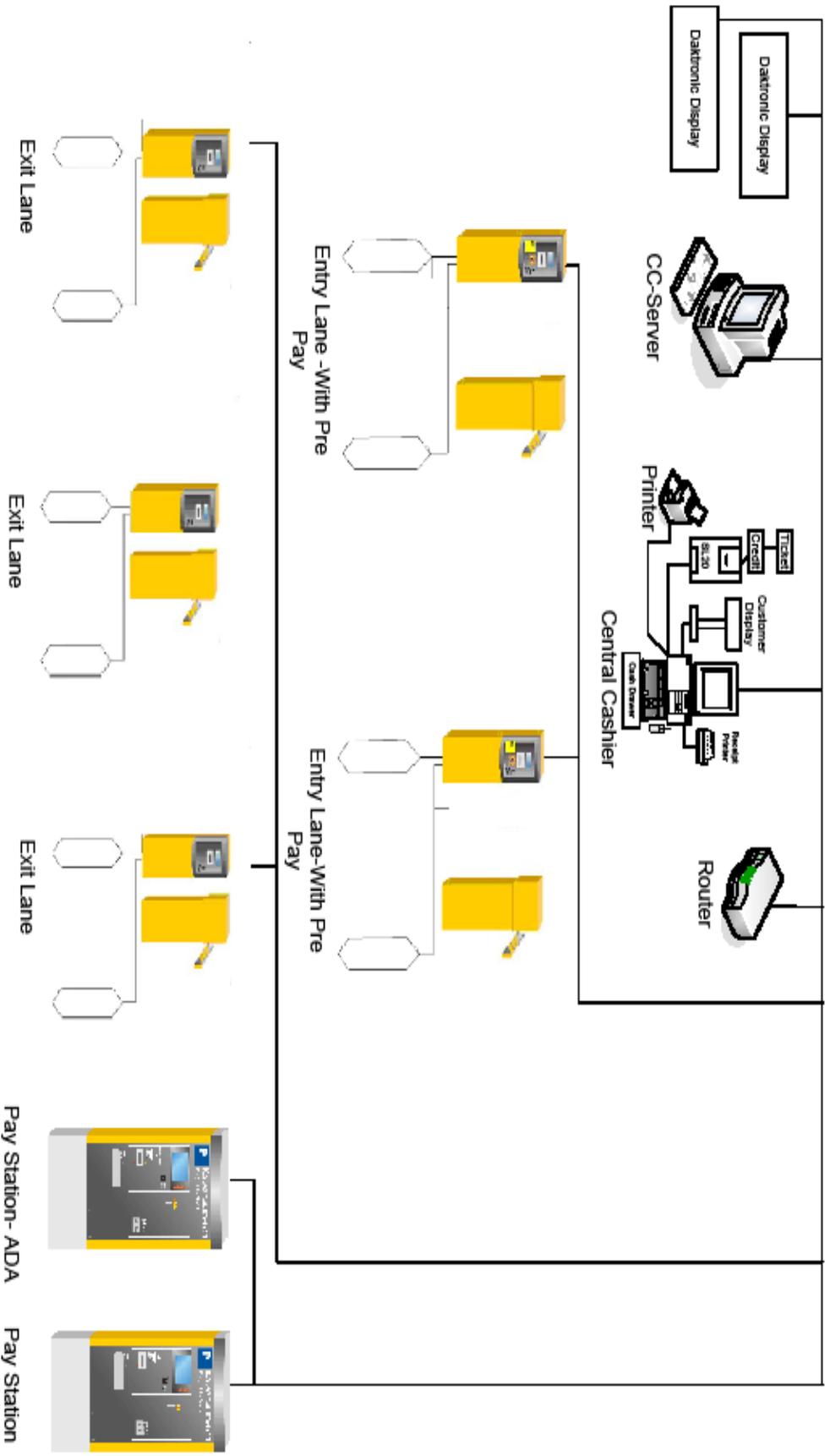
3.3.2 Network Addresses

All network addresses will be provided to Contractor by City.

DEVICE TYPE	Device #	Device Name
POS30	TBD	FC 2 nd /San Carlos
Cisco Router	TBD	TBD
Entry	191	2 nd Street En 1
Entry	192	3 rd Street En 2
ENTRY	291	2 nd Street Exit 1
EXIT	292	2 nd Street Exit 2
EXIT	293	3 rd Street Exit 3
APS	691	PoF 1 2 nd Street -ADA
APS	694	PoF 2 3 rd Street
CC SERV	TBD	Server located at City Hall (City Provided Device)

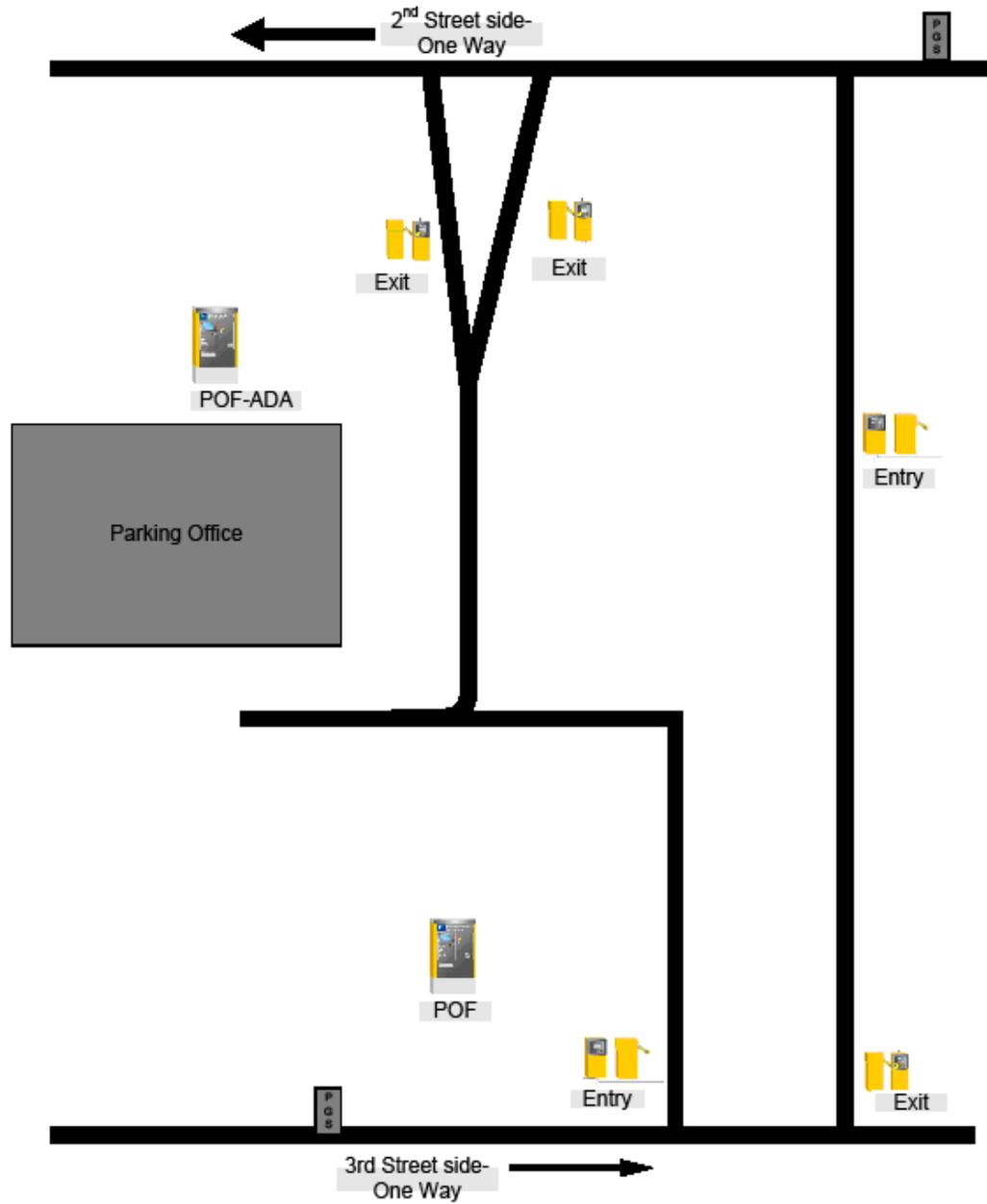
NOTE: TBD items will be identified during the System Design Phase.

3.3.3 System Drawing



Scheidt & Bachmann USA	
2 nd & San Carlos	08/06/2008

3.3.4 System Layout



3.4 LANE EQUIPMENT SETUP

3.4.1 Entry Lane

Position	Description	Available
1	Flashing Ticket Request Button	X
2	Credit Card In/Out	X
3	Backout Detection	X
4	Ticket Retraction by Backout without Ticket	X
5	Illegal Movement detection	N/A
6	Lane Status Light	X
7	Lot Full Sign	N/A
8	Gate Rebound	X
9	Gate open by Power off	X
10	Gate Rebound by Tailgating	X
11	Gate Stop by Tailgating	N/A
12	Pre-pay	X
13	Voice prompt	X
14	Intercom	X
15	HID reader	X
16	Single/Multi use pass	X

3.4.2 Express Exit Lane

Position	Description	Available
1	Flashing Cancel Button	X
2	Credit Card or Coupon Processing	X
3	Credit Card In/Out	X
4	Illegal Movement Detection	N/A
5	Lane Status Light	X
6	Gate Rebound	X
7	Gate open by Power off	X
8	Gate Rebound by Tailgating	X
9	Gate Stop by Tailgating	N/A
10	Voice prompt	X
11	Intercom	X
12	HID reader	X

3.4.3 Pay on Foot

Position	Description	Available
1	Slide Show	X
2	Illuminating Frames	X
3	Journal Printer active on all Transactions	N/A
4	Credit Card Processing	X
5	Special Means of Payments (Special Bitmaps required)	X
6	Voice prompt	X
7	Intercom	X
8	Lost Ticket Button	X
9	Dual Note Dispenser	X
10	1 \$0.25 hopper	X

3.4.4 Central Cashier Station

Position	Description	Available
1	Keyboard Layout (see Section 3.4.5)	X
2	Cash Drawer	X
3	Credit Card Processing	X
4	Lost Ticket & ISF via Grey List	X
5	Detailed Shift Report on Receipt Printer	N/A
6	Event Tariff Active	X
7	Input of Article Numbers allowed	X

3.4.5 Keyboard Layout

Q	W	E	R	T	Y	U	I	O	P	Amnt. Re-ceived	\$ 5	\$ 10	\$ 20	\$ 50	
A	S	D	F	G	H	J	K	L	Rcpt. on/off	Last Rcpt.	← CANCEL →	Check	Manual Credit		
Z	X	C	V	B	N	M	()			DEL	↑	CLEAR	Credit	
\	/	-	+	*	&	#			Void		←	↓	→		
Retail Val.	CBD Val.	Single Use Pass	Multi Use Pass	Timed In/Out Pass	Debit Card				ISF Transaction	ISF payment	7	8	9	Cash	
									Non Rev Trans	Contr. Val	4	5	6		
unread Ticket	Lost Ticket	unread. Val	Stamp Retail Val.								1	2	3	Enter	
			Stamp CBD Val.						Shift Close	Shift Break	0	00	.		

3.4.6 VMS Displays

Contractor shall utilize existing PGS signs currently installed and configure to new Facility controller.

3.5 OPERATIONAL DESCRIPTION FOR PARKING SYSTEMS

The operational description described in this section applies to the parking systems installed at 2nd/San Carlos, as detailed in Sections 3 of this Scope of Services.

3.6 GENERAL

3.6.1 The Scheidt & Bachmann Transaction Parking System is based on a magnetic ISO Side Stripe Parking Ticket. All information necessary to calculate Parking Fees, expired grace times or ticket validity is encoded on the ticket.

3.6.2 The Parking Card Access Control System is interfaced through the industry standard Wiegand Interface. The administration of Monthly Permit Parker is handled through the CMS/S Monthly Parker Administration Software Package.

3.6.3 The Revenue Report Package is based on open and closed Cashier or Machine Shifts. All shifts that are closed between 12:00 Midnight and 12:00 Midnight of the following day, will be combined in the daily Report. The daily Reports will be combined into a Weekly Report after seven (7) days. The weekly reports will be combined into a Monthly Report. The Monthly Reports will be combined into an annual Report.

3.6.4 In addition, the PARCS credit card processing module (CreditPay) working in concert with entry lane devices, exit lane devices, fee computers, credit card server processes, and data handling modules is compliant as mandated by the Visa Payment Application Best Practices: PABP.

3.6.5 The PARCS will provide the enterVo Standard Report Package in addition to the pre-pay and the contractor/manager validation reports.

3.7 TRANSIENT PARKER

3.7.1 Entry Lane. When a Vehicle has triggered the "Presence Loop" of the Ticket Dispenser (PGL30/S) the Dispenser will be activated and is ready for a transaction. The Ticket Request Button flashes, the Backlight of the Display is flashing, the Backlight of the Display is illuminated and a voice prompt informs the patron about options. At this time, the following transactions can be initiated:

3.7.1.1 Request for a transient parking ticket

3.7.1.2 Insertion of a system encoded Pass

3.7.1.3 Presenting of a Proximity Card

3.7.1.4 Insertion of a valid Credit Card (credit card in/out)

3.7.2 The start of any one of the transactions noted above will disable the Dispenser for all other transactions.

3.7.3 Valid Entry. If the presence of a vehicle is sensed at the arming loop and the Ticket request button is pressed, a Transient Ticket is produced. The initially empty magnetic stripe will be encoded with:

3.7.3.1 Facility Code

3.7.3.2 Entry Lane

3.7.3.3 Entry Date & Time

3.7.4 In addition, the Ticket will be imprinted with:

3.7.4.1 Facility Code

3.7.4.2 Entry Lane

3.7.4.3 Entry Time

3.7.4.4 Ticket audit number

3.7.5 After production, the ticket will be placed into the ticket chute. The display text and a voice prompt requesting the patron to remove the ticket. If the ticket is removed the display will show a user programmable welcome message and the Gate opens.

3.7.6 When the vehicle passes the closing loop, a counting impulse is given for a transient parker. The ticket is registered as a valid transient ticket and the gate closes.

3.7.7 Pre-Pay Parking. The operator can switch each Entry Lane individually into a pre-paid mode. This mode can be activated through the Unit Control, through the Service keypad, or use of a key at the Entry Lane.

3.7.7.1 In Pre-pay mode, the Entry Lane will issue a 'Pre-Paid Ticket' that will be encoded with a pre defined exit time (the City defines this time as 6:00 AM the next day). In addition a user defined sales amount is booked into the entry lane shift for each ticket issued. The initially empty magnetic stripe will be encoded with:

3.7.7.1.1 Facility Code

3.7.7.1.2 Entry Lane

3.7.7.1.3 Pre-Paid time

3.7.7.1.4 Entry Time

3.7.7.2 In addition, the Ticket will be imprinted with:

3.7.7.2.1 Facility Code

3.7.7.2.2 Entry Lane

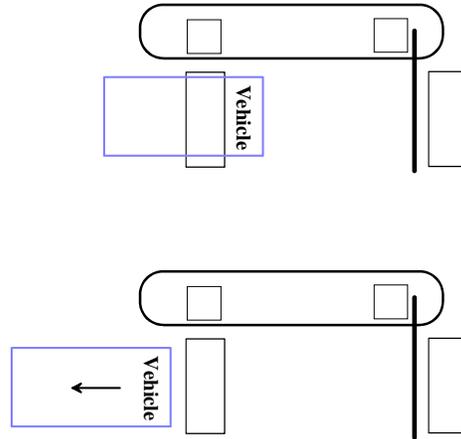
3.7.7.2.3 Entry Date & Time

3.7.7.2.4 Ticket audit number

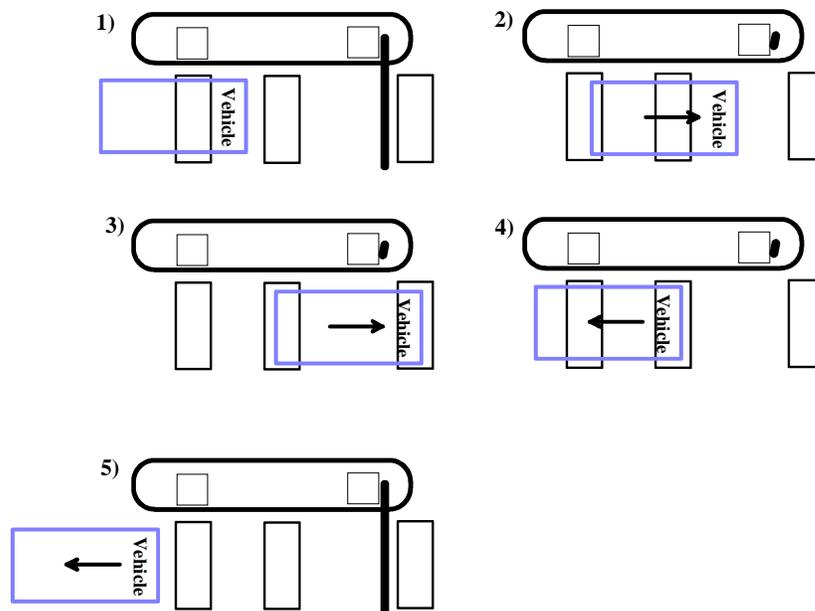
3.7.7.2.5 Pre-pay expired time

3.7.8 Back Out. If a vehicle does not complete the entry movement and is not entering the parking facility it is defined as a back-out transaction. The Scheidt & Bachmann Revenue Control System considers and detects a back-out in two ways.

3.7.9 Two loop back-out detection. If an entry lane is equipped with only two inductive traffic loops the system will consider a back-out if after the ticket is requested and produced the arming loop does not sense a vehicle any longer but the barrier loop does not get a present signal within 4 seconds.



3.7.10 Three loop back-out detection. The City has elected to install two loop Configuration in all Entry lanes. If an entry lane is equipped with three inductive traffic loops the system will consider a back-out if after the ticket is requested and produced the vehicle does not complete the entry movement.



3.7.11 Invalid Entry (Back Out Ticket not taken). If the presence of a vehicle is sensed at the arming loop and the Ticket request button is pressed, a Transient Ticket is produced. The initially empty magnetic stripe will be encoded with:

3.7.11.1 Facility Code

3.7.11.2 Entry Lane

3.7.11.3 Entry Time

3.7.12 In addition, the Ticket will be imprinted with:

3.7.12.1 Facility Code

3.7.12.2 Entry Lane

3.7.12.3 Entry Date & Time

3.7.12.4 Ticket audit number

3.7.13 After production, the ticket will be placed into the ticket chute, the display text and a voice prompt requesting the patron to remove the ticket. If the Patron should back-out of the Lane without taking the Ticket, the Ticket is retracted and electronically marked as invalid.

3.7.14 Invalid Entry (Back Out Ticket taken). If the presence of a vehicle is sensed at the arming loop and the Ticket request button is pressed, a Transient Ticket is produced. The initially empty magnetic stripe will be encoded with:

3.7.14.1 Facility Code

3.7.14.2 Entry Lane

3.7.14.3 Entry Time

3.7.15 In addition, the Ticket will be imprinted with:

3.7.15.1 Facility Code

3.7.15.2 Entry Lane

3.7.15.3 Entry Time

3.7.15.4 Ticket audit number

3.7.16 After production, the ticket will be placed into the ticket chute, the display text and a voice prompt requesting the patron to remove the ticket. If the ticket is removed the display will show a user programmable welcome message and the Gate opens. When the vehicle is leaving the arming loop without crossing the closing loop a "Back-Out Alarm" will sound at the Facility Controller. The ticket is stored by the system as invalid.

3.7.17 Credit Card In/Out. Ticket dispensers are configured with the ability to accept credit cards at the entrance. The patron would insert an approved ISO-compliant credit/debit card into the card slot on the face of the entry lane device.

3.7.18 Pay on Foot Machine Cash/Credit. If a patron walks up to the Pay on Foot Machine located in the 2nd/San Carlos Garage, the following transactions can be initiated:

3.7.18.1 Payment of a Transient Parking Ticket

3.7.18.2 Additional Payments Special Passes

3.7.18.3 Production of a replacement for a Lost ticket

3.7.18.4 Selection of a flat-Event Rate if enabled by operator

3.7.18.5 Payment of a flat rate Transient Ticket enabling the patron to pay the flat rate anytime and exit

3.7.19 The patron has the following payment options:

3.7.19.1 Cash (Coins \$0.25 and \$1.00 and bills \$1.00, \$5.00, \$10.00 and \$20.00)

3.7.19.2 Credit Cards (Visa, MasterCard, Amex and Discover)

3.7.19.3 System Debit Cards

3.7.19.4 Validation coupon

3.7.20 If the patron chooses to pay with a Credit Card, a pre-authorization is automatically requested from the clearing house via a Frame Relay located at the City Office.

3.7.21 Payment Valid Ticket. If the patron inserts a Transient Parking Ticket into the read/write device the Unit will automatically calculate the parking fee due, based on the appropriate rate table.

3.7.22 When the transaction is finalized, the Ticket will be encoded with time of payment and will be imprinted with payment information as follows:

3.7.22.1 Device ID

3.7.22.2 Transaction Number

3.7.22.3 Shift ID

3.7.22.4 Sales information

3.7.22.5 Time of Payment

3.7.23 The Ticket will be issued back to the patron. The Transaction is registered as valid.

3.7.24 Payment Lost Ticket (if enabled by operator). If a patron has lost his parking Ticket he/she can walk up to a Pay Machine and press the "Lost Ticket" button. The Machine will display the correct sales amount for a Lost Ticket. If the fee is paid, the Pay on Foot will produce a replacement Ticket encoded with Facility Code, Production unit and time of payment. It will be imprinted with production time and a user defined Text string "Lost Ticket" The replacement Ticket is issued to the patron and the transaction is stored as valid.

3.7.25 Backout Ticket. If the patron inserts a Ticket stored as invalid into the system, the Pay on Foot will inform the patron with an Error Message that this Ticket is invalid and to contact a Cashier. No transaction is possible with this Ticket.

3.7.26 Exit Verifier. When a Vehicle is arming the presence Loop of the Exit Verifier (PL30SV), the Verifier will be activated and is ready for a Transaction. The backlight of the Display will be illuminated. The start of one of these transactions will disable the Dispenser for all other transactions. At this time the following transaction can be initiated:

3.7.26.1 Insertion of a transient parking ticket

3.7.26.2 Insertion of a Special Pass

3.7.26.3 Presentation of a Proximity Card

3.7.27 The patron has the following payment options:

3.7.27.1 Credit Cards (Visa, MasterCard, Amex and Discover)

3.7.27.2 System Debit Card

3.7.27.3 Validation Coupons

3.7.28 Paid Ticket in Grace Time. If the presence of a Vehicle is sensed at the arming loop and a transient parking ticket is inserted into the read/write device, the information encoded on the magnetic stripe is checked for the last time of payment. If the time of last payment plus the grace time assigned for this Exit is less than the actual System time, the ticket is swallowed, the gate opens, a user pre-defined “goodbye message” is displayed and a pedestrian warning device is triggered. If the vehicle crosses the closing loop a counting impulse is given for a transient ticket and the transaction is registered as valid Exit movement.

3.7.29 Paid Ticket Grace Time Expired. If the presence of a Vehicle is sensed at the arming loop and a transient parking ticket is inserted into the read/write device, the information encoded on the magnetic stripe is checked for last time of payment. If the time of last payment plus the grace time assigned for this Exit is greater than the actual System time, the ticket is parked in a paper switch. The Verifier will calculate the appropriate parking fee based on the correct rate table and last time of payment and will accept all possible means of payment. Once a payment is made, the ticket is swallowed, a receipt is issued, the gate opens, a user pre-defined “goodbye message” is displayed and a pedestrian warning device is triggered. If the vehicle crosses the closing loop a counting impulse is given for a transient ticket and the transaction is registered as valid Exit movement. If no payment process is started within a certain amount of time the ticket will be reissued to the patron and a user pre defined message will be displayed to the patron.

3.7.30 Unpaid Ticket. If the presence of a vehicle is sensed at the arming loop and a transient parking ticket is inserted into the read/write device, the information encoded on the magnetic stripe is checked for last time of payment. If no last payment is encoded to the ticket, the ticket is parked in a paper switch. The Verifier will calculate the appropriate parking fee based on the correct rate table and entry time and will accept all possible means of payment. If a payment is made the ticket is swallowed, a receipt is issued, the gate opens and a user pre-defined “goodbye message” is displayed. If the vehicle crosses the closing loop, a counting impulse is given for a transient ticket and the transaction is registered as valid Exit movement. If no payment process is started within a certain amount of time the ticket will be reissued to the patron and a user pre defined message will be displayed to the patron.

3.7.31 Back-out ticket. If the presence of a vehicle is sensed at the arming loop and a patron inserts a Ticket stored as invalid in the system, the Exit Verifier will inform the patron with an Error Message that this Ticket is invalid and to contact a Cashier. No transaction is possible with this Ticket.

3.7.32 Central Cashier Station. A Parking Attendant can initiate the following Transactions. The start of one of these transactions will disable the Fee Computer for all other transactions.

3.7.32.1 Payment for a transient parking ticket

3.7.32.2 Production of an unreadable Transient Ticket

3.7.32.3 Production of a Lost Ticket

3.7.32.4 Additional payments for special passes

3.7.32.5 Production of Validation Coupons

3.7.32.6 Production of special Passes

3.7.32.7 Production of an ISF Transaction

3.7.32.8 Production of a Contractor Transaction

3.7.33 The patron has the following payment options:

3.7.33.1 Cash

3.7.33.2 Check

3.7.33.3 Credit Cards (Visa , MasterCard, Amex and Discover)

3.7.33.4 Keyed Validations

3.7.33.5 Validation Coupons

3.7.34 Payment Valid Ticket. If the attendant inserts a transient parking ticket into the read/write device, the Fee Computer will automatically calculate the parking fee due, based on the entry time or last payment time using the appropriate rate table. When the transaction is finalized, the Ticket will be encoded with time of payment and will be imprinted with payment information as follows:

3.7.34.1 Device ID

3.7.34.2 Transaction Number

3.7.34.3 Shift ID

3.7.34.4 Sales information

3.7.34.5 Time of Payment

3.7.35 The Ticket will be issued back to the attendant. The Transaction is registered as valid.

3.7.36 Payment of Unreadable Ticket. If the Transient Ticket inserted by the attendant can not be read by the System the Booth Attendant starts the unreadable Ticket Production. After Entry time printed on the Ticket is keyed into the System the Fee Computer will calculate the appropriate Parking Fee. If the payment is made the Fee Computer will produce a replacement ticket encoded with Facility Code, Production unit and time of payment. It will be imprinted with production time, entry Time and a user defined Text string “unreadable Ticket” The replacement Ticket is issued to the attendant. The Replacement Ticket is used by the customer to Exit the Facility.

3.7.37 Payment of Lost Ticket. If the patron informs the Booth Attendant that the Transient Ticket is lost the Attendant starts the Lost Ticket production. After pressing the Lost Ticket key the system will automatically charge an owner/operator programmable flat fee. If the payment is made the Fee Computer will produce a replacement ticket encoded with Facility Code, Production unit and time of payment. It will be imprinted with production time and a user defined Text string “Lost ticket” The replacement Ticket is issued to the attendant. The Replacement Ticket is used by the customer to Exit the Facility.

3.7.38 ISF-Transaction. If the patron informs the booth attendant that he/she has insufficient funds to pay the parking fee the attendant is initiating an ISF-Transaction. The attendant will need to input the following information:

- 3.7.38.1** Last name
- 3.7.38.2** First name
- 3.7.38.3** Street
- 3.7.38.4** Zip code
- 3.7.38.5** City
- 3.7.38.6** Day of birth
- 3.7.38.7** Driver License
- 3.7.38.8** License Plate Number

3.7.39 After the attendant confirms all the information the Fee computer will search the internal ISF-Database for already existing information about the customer. Identifier for the transaction is first name, last name and day of birth.

3.7.40 If a transaction for this person is found, the attendant will be informed about all transaction inside the Database.

3.7.41 If the transaction is completed the receipt printer will issue a double receipt containing all the information including an ISF-ID and a customized text informing the customer about the outstanding payment.

3.7.42 Contractor-Transaction. If the patron informs the booth attendant that he/she does not have sufficient funds to pay the parking fee the attendant is initiating a Contractor-Transaction. The attendant will need to input the following information:

- 3.7.42.1** Last name
- 3.7.42.2** First name
- 3.7.42.3** Street
- 3.7.42.4** Zip code
- 3.7.42.5** City
- 3.7.42.6** Day of birth
- 3.7.42.7** Driver License
- 3.7.42.8** License Plate Number

3.7.43 If the transaction is completed the receipt printer will issue a double receipt containing all the information including a Contractor-ID and a customized text informing the customer about the outstanding payment.

3.7.44 Payment of an ISF. If a customer wants to pay his ISF he will need the ISF ID. The attendant will initiate the transaction and enters the ISF-ID. The Fee Computer will than display the amount due, including an ISF-Service Fee (if enabled) and the payment can be conducted by all available means of payments. The outstanding ISF-Transaction will be stored as paid in the ISF-Database.

3.7.45 Back-out Ticket. If the attendant inserts a Ticket stored as invalid in the system, the Fee Computer will inform the Cashier with an Error Message that this Ticket is invalid. No transaction is possible with this Ticket.

3.7.46 Unreadable Validations. If a patron did receive an electronic Validation or a Validation that this not readable through the system, the bBooth attendant has the ability to manually apply Validations to the transaction via the Cashier keyboard.

3.7.47 Production of Validation Coupons. If the Cashier or Manager logged-on to the Fee Computer has the appropriate access Level, he will be able to produce Validation Coupons. The following Coupons will be available:

3.7.47.1 Retail Validations

3.7.47.2 CBD Validations

3.7.47.3 Cinema Validation

3.7.48 If all necessary information is input, the Fee Computer will produce the coupons. Coupons will be placed into a bin inside the read/write Device if the number of Coupons produced is more than one.

3.7.49 Production of special Passes. If the Cashier or Manager logged-on to the Fee Computer has the appropriate access Level, he will be able to produce Special Passes. The following Passes will be available:

3.7.49.1 Single Use Pass

3.7.49.2 Multi Use Pass

3.7.49.3 Timed In/Out Pass

3.7.50 If all necessary information is input, the Fee Computer will produce the Passes. Passes will be placed into a bin inside the read/write Device if the number of Passes produced is more than one.

3.8 SPECIAL PASSES

3.8.1 Single Use Pass

3.8.1.1 Entry Movement

When a vehicle is arming the presence loop and a Single Use Pass is inserted into the read/write device. The Pass is checked for valid time frame, expiration date and presence status. If the Pass is accepted by the system it is encoded with the entry time. The pass is imprinted with the time the vehicle must leave the facility without being charged. The gate opens and if the vehicle crosses the closing loop the transaction is registered as valid, a counting impulse is given, and the gate closes.

3.8.1.2 Exit Movement

When a vehicle is arming the presence loop and a Single Use Pass is inserted into the read/write device. The Pass is checked for presence status, entry time and time value encoded on the pass. If the entry time plus encoded time value is larger than the actual system time the pass is swallowed and the exit gate does open. If the vehicle crosses the closing loop the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.1.3 Expired Time

When a vehicle is arming the presence loop and a Single Use Pass is inserted into the read/write device. The Pass is checked for presence status, entry time and time value encoded on the pass. If the entry time plus encoded time value is smaller than the actual system time, the Exit Lane Verifier will calculate the appropriate parking fee. If the parking fee is paid by available means of payments the pass is swallowed, a receipt is issued to the patron, and the exit gate opens. If the vehicle crosses the closing loop the transaction is registered as valid, a counting impulse is given, and the gate closes.

3.8.2 Multi Use Pass

3.8.2.1 Entry Movement

When a vehicle is arming the presence loop and a Multi Use Pass is inserted into the read/write device. The Pass is checked for valid time frame, expiration date and presence status. If the Pass is accepted by the system, it is encoded with the entry time. The gate opens and if the vehicle crosses the closing loop, the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.2.2 Exit Movement

When a vehicle is arming the presence loop and a Multi Use Pass is inserted into the read/write device. The Pass is checked for presence status, entry time and expiration date encoded on the pass. If the expiration date/time is larger than the actual system time the pass is encoded as absent and returned to the patron, the exit gate opens. If the vehicle crosses the closing loop, the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.2.3 Expired Pass

When a vehicle is arming the presence loop and a Multi Use Pass is inserted into the read/write device. The Pass is checked for presence status, entry time and expiration date encoded on the pass. If the expiration date/time is smaller than the actual system time, the Exit Lane Verifier will calculate the appropriate parking fee. If the parking fee is paid by available means of payments, the pass is returned and a receipt is issued to the patron, the exit gate opens. If the vehicle crosses the closing loop the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.2.4 Entry Movement, expired Pass

When a vehicle is arming the presence loop and a Multi Use Pass is inserted into the read/write device. The Pass is checked for expiration date and presence status. If the Pass is not accepted by the system, it is returned to the patron and an error message informs the patron the pass is not valid. The gate remains closed. The patron is able to enter the facility by requesting a transient parker ticket.

3.8.3 Timed In/Out Pass

3.8.3.1 Entry Movement

When a vehicle is arming the presence loop and a Timed In/Out Pass is inserted into the read/write device, the Pass is checked for valid time frame, expiration date and presence status. If the Pass is accepted by the system, it is encoded and imprinted with the entry time. The gate opens and, if the vehicle crosses the closing loop, the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.3.2 Exit Movement

When a vehicle is arming the presence loop and a Timed In/Out Pass is inserted into the read/write device, the Pass is checked for presence status, entry time and remaining time value encoded on the pass. If the time value is larger than the actual system time, the pass is encoded as absent and returned to the patron, the exit gate does open. If the vehicle crosses the closing loop the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.3.3 Expired Time

When a vehicle is arming the presence loop and a Timed In/Out Pass is inserted into the read/write device, the Pass is checked for presence status, entry time and remaining time value encoded on the pass. If the time value is smaller than the actual system time the Exit Lane will calculate the appropriate parking fee. If the parking fee is paid by available means of payments the pass is returned and a receipt is issued to the patron, the exit gate opens. If the vehicle crosses the closing loop, the transaction is registered as valid, a counting impulse is given and the gate closes.

3.8.3.4 Entry Movement, expired Pass

When a vehicle is arming the presence loop and a Timed In/Out Pass is inserted into the read/write device, the Pass is checked for expiration date, remaining time value and presence status. If the Pass is not accepted by the system it is returned to the patron and an error message informs the patron the pass is not valid. The gate remains closed. The patron is able to enter the facility by requesting a transient parker ticket.

3.8.4 Monthly Parker

3.8.4.1 Valid Entry

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card passes every check the gate will open. The vehicle then passes over the closing loop and a counting impulse is given for monthly permits and the transaction is registered as a valid entry movement.

3.8.4.2 Invalid Entry – In Pass-Back

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the pass-back the patron will be informed with a user pre-defined error message that he is in pass-back violation.

3.8.4.3 Invalid Entry – Expired Card

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the expiration date check, the patron will be informed with a user pre-defined error message that the permit is expired.

3.8.4.4 Invalid Entry – Blocked Card

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the blocking check, the patron will be informed with a user pre-defined error message that the permit is blocked.

3.8.5 Exit Verifier

3.8.5.1 Valid Exit

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card passes every check, the gate will open and a pedestrian warning device is triggered. As the vehicle passes over the closing loop, a counting impulse is given for monthly permits. The transaction is then registered as a valid exit movement.

3.8.5.2 Invalid Entry – In Pass-Back

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the pass-back check, the patron will be informed with a user pre-defined error message that he is in pass-back violation.

3.8.5.3 Invalid Entry – Expired Card

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the expiration date check, the patron will be informed with a user pre-defined error message that the permit is expired.

3.8.5.4 Invalid Entry – Blocked Card

If a vehicle is present in front of the reader and the proximity card is presented within reading distance, the card will be evaluated based on expiration date, blocking, pass-back, time profile and valid system card. If the card fails the blocking check, the patron will be informed with a user pre-defined error message that the permit is blocked.

3.9 PARKING RATES

3.9.1 Rate requirements will be clarified in the project meetings and programming will be complete by the date of the of the internal FAT Provided that rate structure definitions are provided to the Contractor by the City no later than 6 weeks prior to the commencement of the internal FAT.

3.9.2 Default Parking Rate. This rate table will be used for non-validated parking tickets and Special Passes where a payment is due. The following variables are available; Day Rate, Night Rate, Weekend Rate, Early Bird, Special Event Rate, ten programmable rate steps. Three different Grace Times can be assigned to the Exit Reader, unpaid Ticket, paid Ticket, Traffic Jam

3.9.3 Initial Settings:

Garages	Day(s)	Rates	
		06:00 to 18:00	18:00 to 06:00
2nd /San Carlos	Mon - Fri	\$0.75/20 min, \$15 max	\$3.00 Flat Rate
	Sat	\$0.00	\$3.00 Flat Rate
	Sun	\$0.00	\$3.00 Flat Rate

3.9.4 24 Hour Maximum: 06:00 to 06:00, \$15.00

3.9.5 Day Maximum: 06:00 to 06:00, \$15.00

3.9.6 Evening Maximum: 18:00 to 06:00, \$3.00 flat rate

3.9.7 Days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

3.9.8 Time Periods:

3.9.8.1 Day: 06:00 to 18:00

3.9.8.2 Evening: 18:00 to 06:00

3.9.9 Pre-pay Rate: \$3.00

3.9.10 Shift Close Schedule (Shift Close Schedule will be finalized during the System Design phase.):

3.9.10.1 Facility: 05:59

3.9.10.2 Entries at: 05:59

3.9.10.3 Exits at: 05:59

3.9.11 Holiday Schedule for 2009:

3.9.11.1 Thursday, January 1 - New Year's Day

3.9.11.2 Monday, January 19 - Martin Luther King Jr's Birthday

3.9.11.3 Monday, February 16 - Washington's Birthday (President's Day)

3.9.11.4 Monday, May 25 - Memorial Day

3.9.11.5 Friday, July 3 - Independence Day

3.9.11.6 Monday, September 7 - Labor Day

3.9.11.7 Monday, October 12 - Columbus Day

3.9.11.8 Wednesday, November 11 - Veterans Day

3.9.11.9 Thursday, November 26 - Thanksgiving Day

3.9.11.10 Friday, December 25 - Christmas Day

3.9.11.11 Friday, January 1, 2009 - New Year's Day

3.9.12 Auto Vend Schedule: City will have option to preset start and end times as required.

3.9.13 Validated Parking Rates

3.9.13.1 Validated Parking Rates for 1hr, 2hr, 3hr, 4hr, 5hr, 6hr, one day, and full Validation are available for the Offline Encoder(Supplied to City under previous contract or purchased through change order under this contract) or keyed Validations at the Central Cashier station.

3.9.13.2 Each Encoder is assigned to a specific Validation and issuer. The revenue Reports will identify each validation type in a separate line item within the report

3.9.13.3 Validation requirements will be clarified in project meetings and programming will be completed by the date of the internal Factory Acceptance Test, providing that these rates were confirmed 6 weeks prior to the internal FAT.

3.9.14 CBD Validation. This Validation will be issued as a system Coupon encoded with a money value. It is accepted as payment at the Exit Verifier, Pay on Foot machine and the Central Cashier station. An unlimited number of coupons can be used for payments. If a payment made with a CBD Validation is being canceled at the Exit Verifier, Pay Machine or Central Cashier Station, the device will produce a replacement Coupon

3.9.15 Retail Validation

3.9.15.1 Validation requirements will be clarified in project meetings and programming will be completed by the date of the internal Factory Acceptance Test, providing that these rates were confirmed 6 weeks prior to the internal FAT.

3.9.15.2 This Validation will be issued as a system coupon encoded with a time value. It is accepted as payment at the Exit Verifier, Pay on Foot Machine and the Central Cashier Station. The encoded time value needs to fit the parking rate steps in order to function correctly. Validations are only valid to a maximum amount of two hours. The coupons can only be used once even if the encoded time value is larger than the parking fee due.

3.9.16 Contractor Validation. If the patron informs the booth attendant that he/she qualifies for a contractor Validation, the attendant initiates the Contractor Validation - Transaction. The attendant will need to input the following information:

3.9.16.1 Last name

3.9.16.2 First name

3.9.16.3 Street

3.9.16.4 Zip code

3.9.16.5 City

3.9.16.6 Day of birth

3.9.16.7 Driver License

3.9.16.8 License Plate Number

3.9.17 After the attendant confirms all the information, the Fee computer will search the Database for existing information about the customer. Identifier for the transaction is first name, last name and day of birth.

3.9.18 If information for this person is found, the attendant will be informed about all transaction in the Database.

3.9.19 If the transaction is completed, the receipt printer will issue a double receipt containing all the information including a Transaction-ID and a customized text pre-programmed in the system.

3.9.20 Cinema Validation. This Validation will be available as a system coupon encoded with a time value, from the Offline Encoder, or from keyed Validations at the Central Cashier station. It is accepted as payment at the Exit Verifier, Pay on Foot Machine and the Central Cashier Station. The encoded time value needs to fit the parking rate steps in order to function correctly. Validations are only valid to a maximum amount of three hours and forty minutes. The coupons can only be used once even if the encoded time value is larger than the parking fee due.

3.9.21 Technology Validation. This Validation will be available as a system coupon encoded with a time value, from the Offline Encoder, or from keyed Validations at the Central Cashier station. It is accepted as payment at the Exit Verifier, Pay on Foot Machine and the Central Cashier Station. The encoded time value needs to fit the parking rate steps in order to function correctly. Validations are only valid to a maximum amount of three hours and forty minutes. The coupons can only be used once even if the encoded time value is larger than the parking fee due.

3.9.22 City Hall Validation. This Validation will be available as a system coupon encoded with a time value, from the Offline Encoder, or from keyed Validations at the Central Cashier station. It is accepted as payment at the Exit Verifier, Pay on Foot Machine and the Central Cashier Station. The encoded time value needs to fit the parking rate steps in order to function correctly. Validations are 1 hr, 2 hr, 3 hr, 4 hr and full Validation. The coupons can only be used once even if the encoded time value is larger than the parking fee due.

3.9.23 Non-Revenue Transaction / Manager Validation. If the patron informs the booth attendant that he/she qualifies for a Non-Revenue Transaction, the attendant is initiating the Non-Revenue Transaction. The attendant will need to input the following information:

- 3.9.23.1** Last name
- 3.9.23.2** First name
- 3.9.23.3** Street
- 3.9.23.4** Zip code
- 3.9.23.5** City
- 3.9.23.6** Day of birth
- 3.9.23.7** Driver License
- 3.9.23.8** License Plate Number

3.9.24 After the attendant confirms all the information, the Fee computer will search the Database for already existing information about the customer. Identifier for the transaction is first name, last name and day of birth.

3.9.25 If history for this person is found, the attendant will be informed about all transaction inside the Database.

3.9.26 If the transaction is completed, the receipt printer will issue a double receipt containing all the information including a Transaction-ID and a customized text pre-programmed in the system.

3.10 UPS SYSTEM

3.10.1 Entry and Exit Lanes. Scheidt & Bachmann will use a Novus Alpha II Outdoor UPS system for all Entry and Exit Devices. This UPS will keep the system operational for ca. 20-30 minutes, depending on Lane usage and Battery load. In the Event of a Power failure, the Scheidt & Bachmann system will generate a system Alarm for each Lane to inform the operator of the Power failure event.

3.10.2 Pay on Foot Devices

Scheidt & Bachmann will use a UPS for all automated Pay Machines. This UPS will keep the system operational for up to twenty minutes, depending on Device Usage and Battery Load. Location of the UPS will be determined upon installation. In the Event of a Power failure, the Scheidt & Bachmann system will generate a system Alarm individually for each Lane to inform the operator of the Power failure event.

3.10.3 Computer & Network Equipment

A UPS will back up all Servers, Facility Controller, Central Cashier Station, Intercom and Network Equipment as well. All Windows XP based Devices will initiate an automatic shutdown in the event that the UPS runs low on Battery Power

3.11 INTERCOM SYSTEM

The provided Intercom system is a state-of-the-art system that will identify the location of the caller to the master station located at the Parking Office. If more than one call is placed at the same time, the patron will hear a busy signal. If the master station does not pick up the call, the intercom controller will automatically dial a pre programmed Phone number provided by the City.

3.12 VOICE BOX

All field Equipment delivered under the contract (Entry Units, Exit Verifier and Pay Machines) will be equipped with a programmable voice box. The voice box will (based on the event playback) generate a voice message to communicate with the customer and inform him about the next step.

3.12.1 Entry Lane. As an example the following messages could be used:

Event	Message
Vehicle on arming loop	"Please press button for Ticket or swipe Permit"
Ticket is produced	"Please take the ticket"
Permit or other pass not working	"Your card did not work, please take a Ticket and inform the Lot attendant"

3.12.2 Exit Verifier. As an example the following messages could be used:

Event	Message
Vehicle on arming loop	"Please insert Ticket or swipe Permit"
Additional payment is required	"Please insert Credit Card or Validation Coupon"
Gate opens	"Thank you and have a nice trip"
Permit or other pass not working	"Your card did not work, please take a Ticket and inform the Lot attendant"

3.12.3 Pay Machine. As an example the following messages could be used:

Event	Message
Amount due is displayed	"Please insert Credit Card or Cash to start payment"
Ticket is returned	"Please take the ticket with you to Exit Garage"
Receipt is printed	"Please take your receipt"

3.13 DATA SECURITY

3.13.1 The main objective of Scheidt & Bachmann regarding security is to provide tools for secure capture, transportation, storage & processing of data for a Parking Revenue Control System.

3.13.2 The complete Scheidt & Bachmann PARCS enterVo including entry, exit, fee computers, facility and central computer, credit card server processes, and data handling modules is compliant as mandated by the Visa Payment Application Best Practices (PABP). Scheidt and Bachmann is pursuing Payment Application – Data Security Standards (PA-DSS) certification within the timeline established by the PCI Data Security Standard Council (Council). The current target date is April 2009. The Contractor and City understand that the Council may change this compliance date; and that Contractor will meet the new target date to maintain PA-DSS compliance.

3.13.3 Database. Scheidt & Bachmann utilizes an Oracle database platform in a Windows operating system. Data exchange with a third party system can be accomplished using standard ODBC or through a transfer with pre-defined ASCII data files. Data can only be exported from the Central Database Server (LR). Requirements for data exportation will be finalized during the System Design phase.

3.13.4 Backup. The City IT Department will back up the Oracle database according to the City's best practices for data integrity and protection.

3.14 COMMON UNDERSTANDING OF FAILURE HANDLING

3.14.1 Ticket Jam

A ticket (or credit card) jam does **not** affect the ongoing of the AT. In case of a ticket jam, customer will ensure that S&B receives the ticket for analysis. A ticket jam will only be evaluated when the ticket is made available to S&B for analysis. Tickets that are physically damaged will not be considered. A ticket or credit card is considered to be physically damaged in case of:

3.14.1.1 card is wet,

3.14.1.2 card is ripped

3.14.1.3 card is twisted (dog-ears,...)

3.14.1.4 card is bent greater than ISO 7810 standard limitations (2.5mm including card thickness)

3.15 COMPONENT FAILURE

A single malfunction of a component does **not** affect the ongoing of the ODT. In case of a component malfunction the required remedy action will be documented by the technician. Exchanged parts will be documented in a test plan. The failure will only be taken in account if the exchanged component is defective based on repair analysis.

3.16 FAILURE LEVELS

3.16.1 Failures shall be categorized into one of three different levels:

3.16.1.1 "A" failures will prevent the commercial use of the PARCS in total and shall relate to a restart of the AT.

3.16.1.2 "B" failures will constitute the failure of a single unit device which does not hinder commercial use of the PARCS in total and may be corrected immediately or during a reasonable time period.

3.16.1.3 In case a level "B" failure is detected, the Customer and S&B will have to agree upon the timeline impact of the failure. Failures that are fixed within less than 48 hours shall not extend the test period. Any failure that needs a correction time of more than 48 hours will extend the test period accordingly.

3.16.1.4 "C" failures will constitute minor failures which do not hinder the system operation and do not disturb the end customers. These shall be noted, fixed, and the specific unit or item re-tested. However, a C level failure shall not relate to an interruption of the testing and / or acceptance procedure.

3.17 PROCEDURES

3.17.1 The Contractor will develop and submit to the City for approval, test procedures, with test data forms, that demonstrate that the PARCS equipment and the software furnished and installed function in full compliance with the specifications provided in this contract.

3.17.2 The Contractor will provide all required test equipment and software, and conduct tests in the presence of the City or representative of the City.

3.17.3 The Contractor will furnish a copy of the approved test procedures and submit the test results to the City using approved test data forms.

3.17.4 The City will review the test results for conformance with the requirements of the approved test procedures.

3.17.5 If the PARCS does not function in conformance with PARCS specifications, the City will submit to Contractor a written list of all deficiencies and discrepancies.

3.18 WARRANTY

3.18.1 Contractor warrants that equipment under normal use and service will be free from defects in material and workmanship for the applicable warranty period. The warranty period for hardware shall be one (1) year from the date of Beneficial Use, as defined by the City of San Jose CIP Action Team; and for software shall be one (1) year from the date of the completion of the Final Acceptance Test. If City claims that equipment is non-conforming, City shall (1) promptly notify Contractor in writing of the basis of such nonconformity; (2) follow Contractor's instructions for return of the equipment; and (3) return the equipment freight prepaid to Contractor's designated location. Contractor shall at its own expense, repair or replace all the defective equipment.

3.18.2 Before the expiration of the warranty period, City must notify Contractor in writing if Equipment or Contractor Software does not conform to these warranties. Upon receipt of such notice, Contractor will investigate the warranty claim. If this investigation confirms a valid warranty claim, Contractor will (at its option and at no additional charge to City) repair the defective Equipment or Contractor Software, replace it with the same or equivalent product, or refund the price of the defective Equipment or Contractor Software. Such action will be the full extent of Contractor's liability hereunder. Repaired or replaced product is warranted for the balance of the original applicable warranty period. All replaced products or parts will become the property of Contractor.

3.18.3 Contractor Duties.

3.18.3.1 Preventative maintenance services will include but are not limited to inspection, testing, necessary adjustment, lubrication, part cleaning, and software upgrades. The Contractor will perform all preventive maintenance of the PARCS components to insure that no facility or lane is removed from service during peak hours of operation to be identified by the City. The Contractor shall also provide their preventive maintenance schedules.

3.18.3.2 Routine maintenance services are defined as those problems that do not affect the overall performance of the system but still require attention.

3.18.3.3 Emergency services are defined as any problem that jeopardizes or degrades the performance of the system.

3.18.3.4 After correct notification, Contractor will begin the repair within a response time of 6 hours.

3.18.3.5 To the extent reasonably possible, the Contractor will repair components that have been replaced for maintenance reasons so that the components are available for future maintenance needs.

3.18.3.6 All service will be performed by factory trained and certified personnel.

3.18.3.7 During the first year warranty period following the final system acceptance, the Contractor shall, upon notification by the City of any malfunction, make the necessary repairs, including labor and materials, at the Contractor's expense.

3.18.3.8 The Contractor will warranty all final assembly hardware, parts, materials, workmanship, and all related installation work for a one (1) year period from the date of Beneficial Use, as defined by the City of San Jose CIP Action Team; and all software for a one (1) year period from the completion date of the final system acceptance test.

3.18.3.9 During the warranty period, the Contractor will repair with new material, or replace with new equipment, at no charge, any defective product. During the warranty period, updates and corrections to all equipment and software will be furnished and installed by the Contractor at no charge to the City.

EXHIBIT A-1

Additional Technical and Security Requirements

1. System Availability and Reliability

- 1.1. The Vendor shall take every precaution to ensure that all systems, files, data, equipment, communications, and facilities are reliable.
- 1.2. In the event that a disaster does disrupt the System, the Vendor shall have an up-to-date detailed recovery plan that shall be ready to be implemented so that services are restored within a reasonable timeframe.
- 1.3. The system must be designed to minimize disruption due to failure of one or more components of the system and should be designed in a manner that allows it to be quickly brought back to the state of full operation in the event of a system failure.
- 1.4. In the event of an outage related to any part of the Vendor-maintained system, the City must immediately inform the Vendor of the following information:
 - 1.4.1. Date and time of the outage
 - 1.4.2. Duration of the outage
 - 1.4.3. What aspects of the system were potentially affected during the outage
- 1.5. After notification of an outage, the Vendor must respond with the following information:
 - 1.5.1. Cause and resolution of the outage
 - 1.5.2. Any resulting adverse effects on customer transactions or City data after the resolution of the problem

2. Information Security and Privacy

- 2.1. Vendor will install and maintain a VPN connection for use in troubleshooting and updating the payment application hardware and operating system.
- 2.2. Vendor will install software provided by the City to interface with the City's existing credit card clearinghouse service. Changes to the clearinghouse interface will be quoted separately.
- 2.3. Vendor must provide the City's technical project lead with the administrator's user name and password and a user list for all password protected computers, systems and equipment located in City property, offices and facilities.
- 2.4. Vendor must cooperate with the City in the instances regarding enterVo(Credit Pay) related audits. Additionally, Vendor must provide any required information or documentation for PCI audit only for items identified in attachment titled "Scheidt & Bachmann PCI Responsibility Matrix".
- 2.5. City data must remain confidential. City data cannot be used by the Vendor for reasons other than system implementation, maintenance, updates or troubleshooting services unless approved in writing by the City of San Jose.
- 2.6. Where such items are included in the Vendor's Scope of Work, the Vendor must have an incident response plan in effect that covers processes and procedures for incidents such as, but not limited to,:
 - 2.6.1. Breach of Personal Information
 - 2.6.2. Firewall Breach
 - 2.6.3. Virus Outbreak
- 2.7. Security practices and measures, as it pertains to Credit Pay 3.0 or other items specifically mentioned in Vendor's scope of work, taken to ensure the security of City Parking data, the system and its users must be documented and provided to the City at the City's request.



Exhibit A-2

Payment Card Industry (PCI) Data Security Standard

Responsibility Matrix

The City will be required to certify the parking revenue system under the Payment Card Industry (PCI) Data Security Standard. Since the individual requirements for certification cannot be the sole responsibility of either the Contractor or the City, the following matrix of shared responsibilities is included.

The PCI Security Standards Council periodically updates the PCI Data Security Standard as needed. Therefore this matrix is included in its current state at the time of execution of the contract. The Contractor and City agree to review and update this matrix on an annual basis as part of a maintenance agreement or as required when a new standard is released.

Within 30 days of the execution of this contract the Contractor will provide the City with an updated matrix as indicated in Exhibit A, Section 2.3 Submittals.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1 Establish firewall configuration standards that include the following:	1.1 Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	1.1.1 Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration			City and S&B (if network delivered by S&B)
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			City and S&B (if network delivered by S&B)r
	1.1.2.b. Verify that the diagram is kept current			City and S&B (if network delivered by S&B)
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the Intranet. Verify that the current network diagram is consistent with the firewall configuration standards.			City and S&B (if firewall delivered by S&B)
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	1.1.4 Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components			City and S&B (if firewall delivered by S&B) if covered by maintenance contract
1.1.5 Documented list of services and ports necessary for business	1.1.5 Verify that firewall configuration standards include a documented list of services/ports necessary for business			S&B
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	1.1.6 Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN			City and S&B (if firewall delivered by S&B) if covered by maintenance contract

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	1.1.7.a Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol, and security features implemented			City and S&B (if firewall delivered by S&B) if covered by maintenance contract
	1.1.7.b Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured			
1.1.8 Quarterly review of firewall and router rule sets	1.1.8.a Verify that firewall configuration standards require quarterly review of firewall and router rule sets			City and S&B (if firewall delivered by S&B) if covered by maintenance contract
	1.1.8.b Verify that the rule sets are reviewed each quarter			City and S&B (if firewall delivered by S&B) if covered by maintenance contract
1.1.9 Configuration standards for routers	1.1.9 Verify that firewall configuration standards exist for both firewalls and routers			City and S&B (if firewall /router delivered by S&B)
1.2 Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.	1.2 Select a sample of firewalls/routers 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. The sample should include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment			City and S&B (if firewall /router delivered by S&B)
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall	1.3 Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
configuration should include:				
1.3.1 Restricting inbound Internet traffic to internet protocol (IP) addresses within the DMZ (ingress filters)	1.3.1 Verify that inbound Internet traffic is limited to IP addresses within the DMZ			City and S&B (if firewall /router delivered by S&B)
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ	1.3.2 Verify that internal addresses cannot pass from the Internet into the DMZ			City and S&B (if firewall /router delivered by S&B)
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	1.3.3 Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run NMAP on all TCP ports with "syn reset" or "syn ack" bits set – a response means packets are allowed through even if they are not part of a previously established session)]			City and S&B (if firewall /router delivered by S&B)
1.3.4 Placing the database in an internal network zone, segregated from the DMZ	1.3.4 Verify that the database is on an internal network zone, segregated from the DMZ			City and S&B (if firewall delivered by S&B) if covered by maintenance contract
1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	1.3.5 Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder environment, and that the restrictions are documented			City and S&B (if firewall /router delivered by S&B)
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	1.3.6 Verify that router configuration files are secure and synchronized [for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations]			City and S&B (if firewall /router delivered by S&B)
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	1.3.7 Verify that all other inbound and outbound traffic not covered in 1.2 and 1.3 above is specifically denied			City and S&B (if firewall /router delivered by S&B)
1.3.8 Installing perimeter firewalls	1.3.8 Verify that there are perimeter firewalls installed			City and

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data			S&B (if firewall /router delivered by S&B)
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	1.3.9 Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee			City
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	1.4 To determine that direct access between external public networks and system components storing cardholder data are prohibited, perform the following, <i>specifically</i> for the firewall/router configuration implemented between the DMZ and the internal network:			
1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic	1.4.1 Examine firewall/router configurations and verify there is no direct route inbound or outbound for Internet traffic			City and S&B (if firewall /router delivered by S&B)
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	1.4.2 Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ			City and S&B (if firewall /router delivered by S&B)
1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	1.5 For the sample of firewall/router components above, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading)			City and S&B (if firewall /router delivered by S&B)

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.1 Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			City and S&B (if firewall /router delivered by S&B)
2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.	2.1.1 Verify the following regarding vendor default settings for wireless environments: <ul style="list-style-type: none"> • WEP keys were changed from default at installation, and are changed anytime any one with knowledge of the keys leaves the company or changes positions • Default SSID was changed • Broadcast of the SSID was disabled • Default SNMP community strings on access points were changed • Default passwords on access points were changed • WPA or WPA2 technology is enabled if the wireless system is WPA-capable • Other security-related wireless vendor defaults, if applicable 			City and S&B (if firewall /router delivered by S&B)
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards	2.2.a Examine the organization's system configuration standards for network components, critical servers, and wireless access points, and verify the system configuration standards are consistent with industry-accepted hardening standards as defined, for example, by SANS, NIST, and CIS			City and S&B (if firewall /router delivered by S&B)
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4)			City and S&B (if firewall /router delivered by

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Technology (NIST), and Center for Internet Security (CIS).				S&B
	2.2.c Verify that system configuration standards are applied when new systems are configured			City and S&B (if firewall /router delivered by S&B)
2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	2.2.1 For a sample of system components, critical servers, and wireless access points, verify that only one primary function is implemented per server			S&B
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	2.2.2 For a sample of system components, critical servers, and wireless access points, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service (for example, FTP is not used, or is encrypted via SSH or other technology)			City and S&B (if firewall /router delivered by S&B)
2.2.3 Configure system security parameters to prevent misuse	2.2.3.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for their operating systems, database servers, Web servers, and wireless systems			City
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards			City and S&B (if firewall /router delivered by S&B)
	2.2.3.c For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately			City and S&B (if firewall /router delivered by S&B)
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	2.2.4 For a sample of system components, critical servers, and wireless access points,, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented, support secure configuration, and that only documented functionality is present on the sampled machines			City and S&B (if firewall /router delivered by S&B)

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.</p>	<p>2.3 For a sample of system components, critical servers, and wireless access points,, verify that non-console administrative access is encrypted by:</p> <ul style="list-style-type: none"> • Observing an administrator log on to each system to verify that SSH (or other encryption method) is invoked before the administrator's password is requested • Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally • Verifying that administrator access to the wireless management interface is encrypted with SSL/TLS. Alternatively, verify that administrators cannot connect remotely to the wireless management interface (all management of wireless environments is only from the console) 			<p>City and S&B (if firewall /router delivered by S&B)</p>
<p>2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."</p>	<p>2.4 Perform testing procedures A.1.1 through A.1.4 detailed in Appendix A, "PCI DSS Applicability for Hosting Providers (with Testing Procedures)" for PCI audits of Shared Hosting Providers, to verify that Shared Hosting Providers protect their entities' (merchants and service providers) hosted environment and data.</p>			<p>n/a</p>

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.</p>	<p>3.1 Obtain and examine the company policies and procedures for data retention and disposal, and perform the following</p> <ul style="list-style-type: none"> • Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) • Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data • Verify that policies and procedures include coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers • Verify that policies and procedures include A programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for an audit, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements 			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:</p>	<p>3.2 If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable</p> <p>For each item of sensitive authentication data below, perform the following steps:</p>			City
<p>3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data</p> <p><i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See "Glossary" for additional information.</i></p>	<p>3.2.1 For a sample of system components, critical servers, and wireless access points, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents 			S&B
<p>3.2.2 Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions</p> <p><i>Note: See "Glossary" for additional information.</i></p>	<p>3.2.2 For a sample of system components, critical servers, and wireless access points, examine the following and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs 			S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	<ul style="list-style-type: none"> • Several database schemas • Database contents 			
<p>3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.</p>	<p>3.2.3 For a sample of system components, critical servers, and wireless access points, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents 			S&B
<p>3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p> <p><i>Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).</i></p>	<p>3.3 Obtain and examine written policies and examine online displays of credit card data to verify that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers</p>			S&B and City
<p>3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> • Strong one-way hash functions (hashed indexes) • Truncation • Index tokens and pads (pads must be securely stored) 	<p>3.4.a Obtain and examine documentation about the system used to protect stored data, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that data is rendered unreadable using one of the following methods:</p> <ul style="list-style-type: none"> • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management 			S&B and City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<ul style="list-style-type: none"> Strong cryptography with associated key management processes and procedures <p>The MINIMUM account information that must be rendered unreadable is the PAN.</p> <p><i>If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls."</i></p>	<p>processes and procedures</p> <p>3.4.b Examine several tables from a sample of database servers to verify the data is rendered unreadable (that is, not stored in plain text)</p> <p>3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that cardholder data is rendered unreadable</p> <p>3.4.d Examine a sample of audit logs to confirm that cardholder data is sanitized or removed from the logs</p> <p>3.4.e Verify that cardholder data received from wireless networks is rendered unreadable wherever stored</p>			<p>S&B and City</p> <p>S&B and City</p> <p>S&B and City</p> <p>S&B and City</p>
<p>3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.</p>	<p>3.4.1.a If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local or Active Directory accounts)</p> <p>3.4.1.b Verify that decryption keys are not stored on the local system (for example, store keys on floppy disk, CD-ROM, etc. that can be secured and retrieved only when needed)</p> <p>3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media)</p>			<p>n/a</p> <p>S&B</p> <p>S&B</p>
<p>3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:</p>	<p>3.5 Verify processes to protect encryption keys used for encryption of cardholder data against disclosure and misuse by performing the following:</p>			
<p>3.5.1 Restrict access to keys to the fewest number of custodians necessary</p>	<p>3.5.1 Examine user access lists to verify that access to cryptographic keys is restricted to very few custodians</p>			<p>City</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.5.2 Store keys securely in the fewest possible locations and forms	3.5.2 Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys			S&B
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:	3.6.a Verify the existence of key management procedures for keys used for encryption of cardholder data			City (operational) and S&B (technical)
	3.6.b For Service Providers only: If the Service Provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and service provider)			n/a
	3.6.c Examine the key management procedures and perform the following:			
3.6.1 Generation of strong keys	3.6.1 Verify that key management procedures require the generation of strong keys			S&B
3.6.2 Secure key distribution	3.6.2 Verify that key management procedures require secure key distribution			S&B
3.6.3 Secure key storage	3.6.3 Verify that key management procedures require secure key storage			S&B
3.6.4 Periodic key changes <ul style="list-style-type: none"> As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically At least annually 	3.6.4 Verify that key management procedures require periodic key changes. Verify that key change procedures are carried out at least annually			City
3.6.5 Destruction of old keys.	3.6.5 Verify that key management procedures require the destruction of old keys			City
3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)	3.6.6 Verify that key management procedures require split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.6.7 Prevention of unauthorized substitution of keys	3.6.7 Verify that key management procedures require the prevention of unauthorized substitution of keys			City
3.6.8 Replacement of known or suspected compromised keys	3.6.8 Verify that key management procedures require the replacement of known or suspected compromised keys			City
3.6.9 Revocation of old or invalid keys	3.6.9 Verify that key management procedures require the revocation of old or invalid keys (mainly for RSA keys)			City
3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	3.6.10 Verify that key management procedures require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities			City

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i></p>	<p>4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks</p> <ul style="list-style-type: none"> Verify that strong encryption is used during data transmission For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit Verify that only trusted SSL/TLS keys/certificates are accepted Verify that the proper encryption strength is implemented for the encryption methodology in use 			City - S&B does not transmit over open public networkd. Certified 3 rd -party authorization software required for online authorizations.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	(Check vendor recommendations/best practices)			
<p>4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.</p> <p>If WEP is used, do the following:</p> <ul style="list-style-type: none"> • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address 	<p>4.1.1.a For wireless networks transmitting cardholder data or connected to cardholder environments, verify that appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS</p>			City and S&B (if firewall / wireless router delivered by S&B)
	<p>4.1.1.b If WEP is used, verify</p> <ul style="list-style-type: none"> • it is used with a minimum 104-bit encryption key and 24 bit-initialization value • it is used only in conjunction with Wi-Fi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS • shared WEP keys are rotated at least quarterly (or automatically if the technology is capable) • shared WEP keys are rotated whenever there are changes in personnel with access to keys • access is restricted based on MAC address 			City and S&B (if firewall / wireless router delivered by S&B)
<p>4.2 Never send unencrypted PANs by e-mail.</p>	<p>4.2.a Verify that an email encryption solution is used whenever cardholder data is sent via email</p>		S&B will never send card holder information, encrypted or otherwise, via email.	City
	<p>4.2.b Verify the existence of a policy stating that unencrypted PAN is not to be sent via email</p>			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	4.2.c Interview 3-5 employees to verify that email encryption software is required for emails containing PANs			City

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)</p> <p><i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i></p>	<p>5.1 For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed</p>			<p>City or S&B If part of maintenance contract</p>
<p>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.</p>	<p>5.1.1 For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware</p>			<p>City or S&B If part of maintenance contract</p>
<p>5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>5.2 Verify that anti-virus software is current, actively running, and capable of generating logs</p> <ul style="list-style-type: none"> • Obtain and examine the policy and verify that it contains requirements for updating anti-virus software and definitions • Verify that the master installation of the software is enabled for automatic updates and periodic scans, and that a sample of system components, critical servers, and wireless access points servers have these features enabled • Verify that log generation is enabled and that logs are retained in accordance with company retention policy 			<p>City or S&B If part of maintenance contract</p>

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	6.1.a For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed			City or S&B If part of maintainace contract
	6.1.b Examine policies related to security patch installation to verify they require installation of all relevant new security patches within 30 days			City
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	6.2.a Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities			City
	6.2.b Verify that processes to identify new security vulnerabilities include use of outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2 as new vulnerability issues are found			City
6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.	6.3 Obtain and examine written software development processes to verify that they are based on industry standards and that security is included throughout the life cycle From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			S&B
6.3.1 Testing of all security patches and system and software configuration changes before deployment	6.3.1 All changes (including patches) are tested before being deployed into production			City or S&B If part of maintainace contract

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.3.2 Separate development, test, and production environments	6.3.2 The test/development environments are separate from the production environment, with access control in place to enforce the separation			City or S&B If part of maintainance contract
6.3.3 Separation of duties between development, test, and production environments	6.3.3 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment			City or S&B If part of maintainance contract
6.3.4 Production data (live PANs) are not used for testing or development	6.3.4 Production data (live PANs) are not used for testing and development, or are sanitized before use			City or S&B If part of maintainance contract
6.3.5 Removal of test data and accounts before production systems become active	6.3.5 Test data and accounts are removed before a production system becomes active			City or S&B If part of maintainance contract
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers	6.3.6 Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers			City or S&B If part of maintainance contract
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	6.3.7.a Obtain and review any written or other policies to confirm that code reviews are required and must be performed by individuals other then originating code author			S&B
	6.3.7.b Verify code reviews are conducted for new code and after code changes <i>Note: This requirement applies to code reviews for custom software development, as part of the System Development Life Cycle (SDLC) – these reviews can be conducted by internal personnel. Custom code for web-facing applications will be subject to additional controls as of June 30, 2008 – see PCI DSS requirement 6.6 for details.</i>			S&B
6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:	6.4.a Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	6.4.b For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:			City or S&B If part of maintainance contract
6.4.1 Documentation of impact	6.4.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change			S&B
6.4.2 Management sign-off by appropriate parties	6.4.2 Verify that management sign-off by appropriate parties is present for each sampled change			City and S&B
6.4.3 Testing of operational functionality	6.4.3 Verify that operational functionality testing was performed for each sampled change			City or S&B If part of maintainance contract
6.4.4 Back-out procedures	6.4.4 Verify that back-out procedures are prepared for each sampled change			City or S&B If part of maintainance contract
6.5 Develop all web applications based on secure coding guidelines. such as the <i>Open Web Application Security Project Guidelines</i> . Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:	6.5.a Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the <i>OWASP Guidelines</i> (http://www.owasp.org)			S&B
	6.5.b For any web-based applications, verify that processes are in place to confirm that web applications are not vulnerable to the following			
6.5.1 Unvalidated input	6.5.1 Unvalidated input			S&B
6.5.2 Broken access control (for example, malicious use of user IDs)	6.5.2 Malicious use of User IDs			S&B
6.5.3 Broken authentication and session management (use of account credentials and session cookies)	6.5.3 Malicious use of account credentials and session cookies			n/a
6.5.4 Cross-site scripting (XSS) attacks	6.5.4 Cross-site scripting			S&B
6.5.5 Buffer overflows	6.5.5 Buffer overflows due to unvalidated input and other causes			S&B
6.5.6 Injection flaws (for example,	6.5.6 SQL injection and other command injection flaws			S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
structured query language (SQL) injection)				
6.5.7 Improper error handling	6.5.7 Error handling flaws			S&B
6.5.8 Insecure storage	6.5.8 Insecure storage			S&B
6.5.9 Denial of service	6.5.9 Denial of service			S&B
6.5.10 Insecure configuration management	6.5.10 Insecure configuration management			S&B
<p>6.6 Ensure that all web-facing applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application-layer firewall in front of web-facing applications <p><i>Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.</i></p>	<p>6.6 For web-based applications, ensure that one of the following methods are in place as follows:</p> <ul style="list-style-type: none"> • Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections • Verify that an application-layer firewall is in place in front of web-facing applications to detect and prevent web-based attacks 			n/a

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement ensures critical data can only be accessed by authorized personnel.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.</p>	<p>7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:</p> <ul style="list-style-type: none"> • Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities • Assignment of privileges is based on individual personnel's job classification and function • Requirement for an authorization form signed by management that specifies required privileges • Implementation of an automated access control system 			City
<p>7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.</p>	<p>7.2 Examine system settings and vendor documentation to verify that an access control system is implemented and that it includes the following</p> <ul style="list-style-type: none"> • Coverage of all system components • Assignment of privileges to individuals based on job classification and function • Default "deny-all" setting (some access control systems are set by default to "allow-all" thereby permitting access unless/until a rule is written to specifically deny it) 			City

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.	8.1 For a sample of user IDs, review user ID listings and verify that <u>all</u> users have a unique username for access to system components or cardholder data			City
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> • Password • Token devices (for example, SecureID, certificates, or public key) • Biometrics 	8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder environment, perform the following: <ul style="list-style-type: none"> • Obtain and examine documentation describing the authentication method(s) used • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s) 			City
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	8.3 To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (Smart card, token PIN) are required.			City and S&B
8.4 Encrypt all passwords during transmission and storage on all system components.	8.4.a For a sample of system components, critical servers, and wireless access points, examine password files to verify that passwords are unreadable			S&B
	8.4.b For Service Providers only, observe password files to verify that customer passwords are encrypted			S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	8.5 Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	8.5.1.a Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following: <ul style="list-style-type: none"> • Obtain and examine an authorization form for each ID • Verify that the sampled User IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained,.), by tracing information from the authorization form to the system 			City
	8.5.1.b Verify that only administrators have access to management consoles for wireless networks			City
8.5.2 Verify user identity before performing password resets	8.5.2 Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, email, web, or other non-face-to-face method, the user's identity is verified before the password is reset			City
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	8.5.3 Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use			City
8.5.4 Immediately revoke access for any terminated users	8.5.4 Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been inactivated or removed			City
8.5.5 Remove inactive user accounts at least every 90 days	8.5.5 For a sample of user IDs, verify that there are no inactive accounts over 90 days old			City
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	8.5.6 Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used			City
8.5.7 Communicate password procedures and policies to all	8.5.7 Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
users who have access to cardholder data				
8.5.8 Do not use group, shared, or generic accounts and passwords	8.5.8.a For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following <ul style="list-style-type: none"> • Generic User IDs and accounts are disabled or removed • Shared User IDs for system administration activities and other critical functions do not exist • Shared and generic User IDs are not used to administer wireless LANs and devices 			City
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited			City
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested			City
8.5.9 Change user passwords at least every 90 days	8.5.9 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change			City S&B
8.5.10 Require a minimum password length of at least seven characters	8.5.10 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements			City S&B
8.5.11 Use passwords containing both numeric and alphabetic characters	8.5.11 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters For Service Providers only, review internal processes and			City S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used	8.5.12 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords For Service Providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords			City S&B
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	8.5.13 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts For Service Providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts			City S&B
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	8.5.14 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account			S&B
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	8.5.15 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less			S&B
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	8.5.16.a Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators			S&B
	8.5.16.b Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts. Direct SQL queries should be limited to database administrators)			S&B

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data <ul style="list-style-type: none"> Verify that access is controlled with badge readers and other devices including authorized badges and lock and key Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use 			City
9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	9.1.1 Verify that video cameras monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Verify that cameras are monitored and that data from cameras is stored for at least three months			City
9.1.2 Restrict physical access to publicly accessible network jacks	9.1.2 Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks			City
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	9.1.3 Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted			City
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. <i>"Employee" refers to full-time and part-time employees, temporary</i>	9.2.a Review processes and procedures for assigning badges to employees, contractors, and visitors, and verify these processes include the following: <ul style="list-style-type: none"> Procedures in place for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges Limited access to badge system 			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<i>employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>	9.2.b Observe people within the facility to verify that it is easy to distinguish between employees and visitors			City
9.3 Make sure all visitors are handled as follows:	9.3 Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	9.3.1 Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data			City
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	9.3.2 Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outside and that visitor badges expire			City
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	9.3.3 Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration			City
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.	9.4.a Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted			City
	9.4.b Verify that the log contains the visitor’s name, the firm represented, and the employee authorizing physical access, and is retained for at least three months			City
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility.	9.5 Verify that the storage location for media backups is secure. Verify that offsite storage is visited periodically to determine that backup media storage is physically secure and fireproof			City
9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications	9.6 Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media in computer rooms and data centers (including paper receipts, paper reports, faxes, CDs, and disks in employee desks and open			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data	workspaces, and PC hard drives)			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: including the following	9.7 Verify that a policy exists to control distribution of media containing cardholder data, that the policy covers all distributed media including that distributed to individuals			City
9.7.1 Classify the media so it can be identified as confidential	9.7.1 Verify that all media is classified so that it can be identified as "confidential"			City
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	9.7.2 Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery mechanism that can be tracked			City
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	9.8 Select a recent sample of several days of offsite media tracking logs, and verify the presence in the logs of tracking details and proper management authorization			City
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	9.9 Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.			City
9.9.1 Properly inventory all media and make sure it is securely stored.	9.9.1.a Obtain and review the media inventory log to verify that periodic media inventories are performed 9.9.1.b Review processes to verify that media is securely stored			
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows	9.10 Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:			City
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials	9.10.1.a Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped, in accordance with ISO 9564-1 or ISO 11568-3e			City
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	to its contents			
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed	9.10.2 Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media			City

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active, including for any connected wireless networks.			City
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Verify through interviews, examination of audit logs, and examination of audit log settings, that the following events are logged into system activity logs:			
10.2.1 All individual accesses to cardholder data	10.2.1 All individual access to cardholder data			S&B
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Actions taken by any individual with root or administrative privileges			City and S&B
10.2.3 Access to all audit trails	10.2.3 Access to all audit trails			City and S&B
10.2.4 Invalid logical access attempts	10.2.4 Invalid logical access attempts			City and S&B
10.2.5 Use of identification and authentication mechanisms	10.2.5 Use of identification and authentication mechanisms			City and S&B
10.2.6 Initialization of the audit logs	10.2.6 Initialization of audit logs			City and S&B
10.2.7 Creation and deletion of system-	10.2.7 Creation and deletion of system level objects			City and S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
level objects				
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Verify through interviews and observation, for each auditable event (from 10.2), that the audit trail captures the following:			
10.3.1 User identification	10.3.1 User identification			City and S&B
10.3.2 Type of event	10.3.2 Type of event			City and S&B
10.3.3 Date and time	10.3.3 Date and time stamp			City and S&B
10.3.4 Success or failure indication	10.3.4 Success or failure indication, including those for wireless connections			City and S&B
10.3.5 Origination of event	10.3.5 Origination of event			City and S&B
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Identity or name of affected data, system component, or resources			City and S&B
10.4 Synchronize all critical system clocks and times	10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:			S&B
	10.4.a Verify that NTP or similar technology is used for time synchronization			City and S&B
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]			S&B
	10.4.c Verify that the Network Time Protocol (NTP) is running the most recent version			City and S&B

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	<p>10.4.d Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information</p>			City and S&B
<p>10.5 Secure audit trails so they cannot be altered</p>	<p>10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:</p>			
<p>10.5.1 Limit viewing of audit trails to those with a job-related need</p>	<p>10.5.1 Verify that only individuals who have a job-related need can view audit trail files</p>			City and S&B
<p>10.5.2 Protect audit trail files from unauthorized modifications</p>	<p>10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation</p>			City and S&B
<p>10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.</p>	<p>10.5.3 Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter</p>			City and S&B
<p>10.5.4 Copy logs for wireless networks onto a log server on the internal LAN</p>	<p>10.5.4 Verify that logs for wireless networks are offloaded or copied onto a centralized internal log server or media that is difficult to alter</p>			City
<p>10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)</p>	<p>10.5.5 Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities</p>			City
<p>10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and</p>	<p>10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required</p>			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
accounting protocol (AAA) servers (for example, RADIUS). <i>Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6</i>	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components			City
10.7 Retain audit trail history for at least one year, with a minimum of three months available online.	10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year			City
	10.7.b Verify that audit logs are available online or on tape for at least one year			City

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	11.1.a Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.			City
	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.			n/a
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	11.2.a Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Verify that the scan process includes rescans until “clean” results are obtained			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p><i>Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.</i></p>	<p>11.2.b To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify that</p> <ul style="list-style-type: none"> • Four quarterly scans occurred in the most recent 12-month period • The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures 			City
<p>11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following</p>	<p>11.3 Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that any noted vulnerabilities were corrected. Verify that the penetration tests include:</p>			City
<p>11.3.1 Network-layer penetration tests</p>	<p>11.3.1 Network-layer penetration tests</p>			City
<p>11.3.2 Application-layer penetration tests</p>	<p>11.3.2 Application-layer penetration tests</p>			City
<p>11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.</p>	<p>11.4.a Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored</p>			City
	<p>11.4.b Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises</p>			City
	<p>11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection</p>			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.</p> <p><i>Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider)</i></p>	<p>11.5 Verify the use of file integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities</p>			City

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
<p>12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:</p>	<p>12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners)</p>			City
<p>12.1.1 Addresses all requirements in this specification</p>	<p>12.1.1 Verify that the policy addresses all requirements in this specification.</p>			City
<p>12.1.2 Includes an annual process</p>	<p>12.1.2 Verify that the information security policy includes</p>			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
that identifies threats, and vulnerabilities, and results in a formal risk assessment	an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment			
12.1.3 Includes a review at least once a year and updates when the environment changes	12.1.3 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment			City
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	12.2.a Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements			City
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	12.3 Obtain and examine the policy for critical employee-facing technologies and verify the policy contains the following:			
12.3.1 Explicit management approval	12.3.1 Verify that the usage policies require explicit management approval to use the devices			City
12.3.2 Authentication for use of the technology	12.3.2 Verify that the usage policies require that all device use is authenticated with username and password or other authentication item (for example, token)			City
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices			City
12.3.4 Labeling of devices with owner, contact information, and purpose	12.3.4 Verify that the usage policies require labeling of devices with owner, contact information, and purpose			City
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies require acceptable uses for the technology			City
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies require acceptable network locations for the technology			City
12.3.7 List of company-approved products	12.3.7 Verify that the usage policies require a list of company-approved products			City
12.3.8 Automatic disconnect of	12.3.8 Verify that the usage policies require automatic			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
modem sessions after a specific period of inactivity	disconnect of modem sessions after a specific period of inactivity			
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use	12.3.9 Verify that the usage policies require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use			City
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access	12.3.10 Verify that the usage policies prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem. Verify that the policies prohibit cut-and-paste and print functions during remote access			City
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	12.4 Verify that information security policies clearly define information security responsibilities for both employees and contractors			City
12.5 Assign to an individual or team the following information security management responsibilities:	12.5 Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			City
12.5.1 Establish, document, and distribute security policies and procedures	12.5.1 Verify that responsibility for creating and distributing security policies and procedures is formally assigned			City
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel	12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned			City
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	12.5.3 Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned			City
12.5.4 Administer user accounts,	12.5.4 Verify that responsibility for administering user			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
including additions, deletions, and modifications	account and authentication management is formally assigned			
12.5.5 Monitor and control all access to data	12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned			City
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:	12.6.a Verify the existence of a formal security awareness program for all employees			City
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)			City
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually			City
12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures	12.6.2 Verify that the security awareness program requires employees to acknowledge in writing that they have read and understand the company's information security policy			City
12.7 Screen potential employees to minimize the risk of attacks from internal sources. <i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	12.7 Inquire of Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential employees who will have access to cardholder data or the cardholder data environment. (Examples of background checks include pre-employment, criminal, credit history, and reference checks)			City
12.8 If cardholder data is shared with service providers, then contractually the following is required:	12.8 If the audited entity shares cardholder data with another company, obtain and examine contracts between the organization and any third parties that handle cardholder data (for example, backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes). Perform the following:			
12.8.1 Service providers must	12.8.1 Verify that the contract contains provisions requiring			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
adhere to the PCI DSS requirements	adherence to the PCI DSS requirements			
12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses	12.8.2 Verify that the contract contains provisions for acknowledgement by the third party of their responsibility for securing cardholder data			City
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.9 Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)	12.9.1 Verify that the Incident Response Plan and related procedures include <ul style="list-style-type: none"> • roles, responsibilities, and communication strategies in the event of a compromise • coverage and responses for all critical system components • notification, at a minimum, of credit card associations and acquirers • strategy for business continuity post compromise • reference or inclusion of incident response procedures from card associations • analysis of legal requirements for reporting compromises (for example, per California bill 1386, notification of affected consumers is a requirement in the event of an actual or suspected compromise, for any business with California residents in their database) 			City
12.9.2 Test the plan at least annually	12.9.2 Verify that the plan is tested at least annually			City
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts	12.9.3 Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes			City
12.9.4 Provide appropriate training to staff with security breach	12.9.4 Verify through observation and review of policies that staff with security breach responsibilities are			City

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
response responsibilities	periodically trained			
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	12.9.5 Verify through observation and review of processes that monitoring and responding to alerts from security systems are included in the Incident Response Plan			City
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	12.9.6 Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments			City
12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following	12.10 Verify through observation, review of policies and procedures, and review of supporting documentation that there is a process to manage connected entities by performing the following:			
12.10.1 Maintain list of connected entities	12.10.1 Verify that a list of connected entities is maintained			City
12.10.2 Ensure proper due diligence is conducted prior to connecting an entity	12.10.2 Verify that procedures ensure that proper due diligence is conducted prior to connecting an entity			City
12.10.3 Ensure the entity is PCI DSS compliant	12.10.3 Verify that procedures ensure that the entity is PCI DSS compliant			City
12.10.4 Connect and disconnect entities by following an established process	12.10.4 Verify that connecting and disconnecting entities occurs following an established process			City

EXHIBIT B COMPENSATION

The terms of payment shall be net thirty days from the date of invoice, with invoicing to occur upon certification from contractor that it has successfully completed the following milestones:

PCI/CMS 30 (enterVo) UPGRADE PROJECT

PHASE OF PROJECT	DELIVERABLE or MILESTONE	% OF TOTAL	AMOUNT
Finalized Project Schedule	Finalized Project Schedule	5%	\$19,952
Completion of System Design Document	City Acceptance of SDD	15%	\$59,855
Server & Equipment Acquisition	City Acceptance of Bill of Materials & Delivery On-site of Materials	15%	\$59,855
Substantial Completion of Upgrades at All Facilities	City Acceptance of Notice of Completion	30%	\$119,710
Completion of 30 Day Acceptance Test	City Acceptance of Executed 30 Day Acceptance Test	25%	\$99,759
Project Close out and Final Acceptance	Completion and Acceptance by City of all outstanding deliverables	10%	\$39,904
		100%	\$399,035

PCI-Specific Maintenance

Included: Windows Security patching, Oracle critical patch updates, and Antivirus maintenance for all Scheidt & Bachmann systems. This pricing shall become effective following the initial twelve-month warranty period as required in Exhibit B, Scope of Services. A separate Purchase Order will be issued for each year at the discretion of the City.

Year 1: \$ 38,445.00

Year 2: \$ 40,367.25

Year 3: \$ 43,192.96

Year 4: \$ 47,080.32

2nd/SAN CARLOS PARCS PROJECT

PHASE OF PROJECT	DELIVERABLE or MILESTONE	% OF TOTAL	AMOUNT
Completion of Project Schedule	City Acceptance of Project Schedule	10%	\$27,611
Submittal of Bill of Materials and Delivery of Materials On-site	City Acceptance of BOM & Delivery of materials On-site	20%	\$55,223
Completion of Installation Test	City Acceptance of Executed Installation Test	30%	\$82,834
Completion of 30 Day Acceptance Test	City Acceptance of Executed 30 Day Acceptance Test	30%	\$82,834
Project Close out and Final Acceptance	Completion and Acceptance by City of all outstanding deliverables	10%	\$27,611
		100%	\$276,113

City shall have the option to issue a separate Purchase Order for ongoing maintenance, service and support for the 2nd/San Carlos PARCS equipment each year following the end of the warranty period. City may elect to include the ongoing maintenance, service and support for this facility in its Purchase Order for the maintenance, service and support agreement for all Contractor supported equipment at City's other facilities as well.

All Payments are based upon City's acceptance of Contractor's performance of the phase as evidenced by successful completion of the Deliverable for that Phase. City shall have no obligation to pay unless Contractor has successfully completed and City has approved the Project Phase for which payment is due.

The maximum amount of compensation to be paid to Contractor, including both payment for professional services and reimbursable expenses, shall not exceed Six Hundred Seventy five Thousand One Hundred Forty-eight Dollars (\$675,148). Any hours worked or additional hardware provided for which payment would result in a total exceeding the maximum amount of compensation set forth herein shall be at no cost to City.

**EXHIBIT B-1
MASTER PRICE LIST OF EQUIPMENT,
SOFTWARE AND SERVICES**

Note: All pricing in U.S. dollars

Name of Firm: Scheidt & Bachmann USA, Inc.

Hardware, Software and Services	Part/Component/Description/Details	Quantity	Unit Price	Extended Price
PARCS Upgrade w/PC Hardware (PCI)				
Server/Additional Computer Equipment				
LR	Dell PowerEdge 1950 , Server 2003	1	\$ 7,778.00	\$ 7,778.00
LDS	Dell PowerEdge 2950 , Server 2003	1	\$ 9,904.00	\$ 9,904.00
ZR	Dell PowerEdge 1950 , Server 2003	1	\$ 7,778.00	\$ 7,778.00
LAR	Dell Optiplex 745 SFF	1	\$ 1,451.00	\$ 1,451.00
ZR/POS Combo	Dell Optiplex 745 Desktop XP Professional	5	\$ 1,451.00	\$ 7,255.00
Central Cashier / Encoding	Dell Optiplex 745 Desktop XP Professional	3	\$ 1,451.00	\$ 4,353.00
Exit Cashier Station	Dell Optiplex 745 Desktop XP Professional	2	\$ 1,451.00	\$ 2,902.00
Credit Card Server	Dell PowerEdge 860 w/Windows 2003 Server	1	\$ 2,680.00	\$ 2,680.00
Sub total Additional Computer Eq.				\$ 44,101.00
Field Equipment Software Upgrade to CMS 30				
	CMS 30 LR Software	1	\$ 7,150.00	\$ 7,150.00
	CMS 30 LDS Software	1	\$ 5,280.00	\$ 5,280.00
	CMS 30 ZR	1	\$ 5,500.00	\$ 5,500.00
	CMS 30 ZR/POS Combo	5	\$ 5,940.00	\$ 29,700.00
	CMS 30 LAR	1	\$ 3,300.00	\$ 3,300.00
	CMS 30 Credit Card Server	1	\$ 5,280.00	\$ 5,280.00
	CMS 30 Exit Cashier Station	2	\$ 3,080.00	\$ 6,160.00
	CMS 30 Central Cashier / Encode.	3	\$ 3,080.00	\$ 9,240.00
	CMS 30 Entry/Card Reader/AVI	21	\$ 550.00	\$ 11,550.00
	CMS 30 Exp Exit/Card Reader/AVI	26	\$ 550.00	\$ 14,300.00
	CMS 30 POF	16	\$ 550.00	\$ 8,800.00
	CMS 30 PAY20	4	\$ 550.00	\$ 2,200.00
	Software Installation	1	\$ 64,800.00	\$ 64,800.00
	Hardware Installation	1	\$ 5,625.00	\$ 5,625.00
Sub total Field Equipment Upgrade to CMS 30				\$ 178,885.00
Additional Services/Software Licenses				
	Oracle 10g Standard Ed. One	2	\$ 5,400.00	\$ 10,800.00
	Training (Admin Only, 4-hour session)	6	\$ 900.00	\$ 5,400.00
	Training (Travel, Lodging, etc...)	1	\$ 3,250.00	\$ 3,250.00
	Project Management	1	\$ 25,136.00	\$ 25,136.00
	Off Site installation and testing (\$/day)	5	\$ 1,800.00	\$ 9,000.00
	Off Site Testing (Misc. Expenses)	1	\$ 3,375.00	\$ 3,375.00
	FAT setup and labor (\$/day)	2	\$ 1,800.00	\$ 3,600.00
	FAT (Misc. Expenses)	1	\$ 4,175.00	\$ 4,175.00
	Norton AntiVirus - Corporate License	15	\$ 51.00	\$ 765.00
	EPR 6 Embedded Boards	10	\$ 2,200.00	\$ 22,000.00
	USB Control Boxes	10	\$ 821.00	\$ 8,210.00
	Update Server Configuration	1	\$ 675.00	\$ 675.00
	Cisco VPN / Firewall Hardware & Config.	1	\$ 975.00	\$ 975.00
	ELO 15" POS Touchscreen & Software	10	\$ 1,069.00	\$ 10,690.00
	ICVerify Configuration and Certification Testing	1	\$ 1,800.00	\$ 1,800.00
	One Year Warranty Services	1	\$ 23,565.00	\$ 23,565.00
	System Design and Customization	1	\$ 9,426.00	\$ 9,426.00

Additional Mobilization Costs	1	\$ 6,500.00	\$ 6,500.00
CMS 30 System Documentation (included no cost)		\$ -	\$ -
Sub total Additional Services/Software Licenses			\$ 149,342.00
Tax 8.25% on equipment only			\$ 26,707.26
Sub-Total PARCS Upgrade w/PC Hardware (PCI):			\$ 399,035.26

2nd /San Carlos Garage

Cashier/Cell Computer	Facility Controller /Cashier Computer with Point of Sale Functionality (including fee display & receipt printer)	1	\$ 20,189.00	\$	20,189.00
Network Equipment	Network Equipment (including routers & switches)	1	\$ 2,457.00	\$	2,457.00
Intercom	Commend Intercom System (including 1 master station, routers)	1	\$ 4,185.00	\$	4,185.00
PKA30S	PKA20/S w/ single bill dispenser, bill acceptor, coin processing, \$1.00 & \$.25 Hoppers, voice prompt, pin-hole camera, 1ADA)	2	\$ 41,626.00	\$	83,252.00
Entry Lanes #1 & #2	Ticket Issuing Machine (including HID reader, EM6, pre-pay key, & Voice prompt)	2	\$ 11,236.00	\$	22,472.00
Exit Lanes #1, #2, & #3	Exit Verifier (w/ HID Reader, EM6, Voice prompts, pin hole camera)	3	\$ 12,500.00	\$	37,500.00
AS30	Barrier Gates (including articulated gate arms)	5	\$ 3,619.00	\$	18,095.00
Novus	UPS	8	\$ 1,300.00	\$	10,400.00
	Pedestrian Warning System (including flashing light and audible option)	2	\$ 1,500.00	\$	3,000.00
Others	Shipping	1	\$ 4,650.00	\$	4,650.00
	Installation	1	\$ 55,300.00	\$	55,300.00
	Tax 8.25% on equipment only			\$	14,612.38
Sub-Total 2nd/San Carlos Garage:				\$	276,112.38

Notes:

City of San Jose "Validation Software" included (i.e. Retail, CBD etc)
 Installation includes CAT 5 communication and bolt down of all units
 Includes Vehicle Loop Detectors (New loops in ground not included)
 Report package to mirror current package provided by S & B to the City of San Jose
 All equipment to be RAL 1003 - Standard Yellow
 Credit Card clearing house and associated (dedicated) line provided by Owner
 Does not include any concrete/island modification
 Installation Scope of Work - Turn-Key

Includes:

Installation of 3 exits lanes and all equipment within the lane. This includes new conduit when necessary.
 Installation of a complete intercom system, testing and Configuration
 Includes communication wiring back to the parking office
 Installation of 2 Exit Lanes
 Includes new conduit to pay-stations and inter-island where appropriate
 Installation of 2 Pay on Foot Stations
 Installation and termination of communications cabinet in the parking office
 Installation, configuration of all S & B PARCS software
 30 day Operational Demonstration Test included
 Includes a complete set of As-Built drawings upon completion of installation.

Summary

PARCS Upgrade w/PC Hardware (PCI)

Server/Additional Computer Equipment	\$	44,101.00
Field Equipment Software Upgrade to CMS 30	\$	178,885.00
Additional Services/Software Licenses	\$	149,342.00
<hr/>		
Total before tax	\$	372,328.00
Tax 8.25%	\$	26,707.26
<hr/>		
Total PARCS Upgrade w/PC Hardware (PCI)\	\$	399,035.26

2nd /San Carlos Garage

Equipment Sub total	\$	201,550.00
Shipping	\$	4,650.00
Installation	\$	55,300.00
<hr/>		
Total before tax	\$	261,500.00
Tax 8.25%	\$	14,612.38
<hr/>		
Total 2nd/San Carlos Garage	\$	276,112.38
<hr/>		
Total Project Amount including Tax and Shipping	\$	675,147.64

EXHIBIT C

INSURANCE REQUIREMENTS

INSURANCE REQUIREMENTS. Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from, or in connection with, the performance of the work hereunder by the Contractor, his agents, representatives, employees or subcontractors. The cost of such insurance shall be included in the Contractor's bid.

D-1 Minimum Scope of Insurance

Coverage shall be at least as broad as:

1. The coverage provided by Insurance Services Office Commercial General Liability coverage "occurrence" form CG 0001; and
2. The coverage provided by Insurance Services Office form number CA 0001 covering Automobile Liability. Coverage shall be included for all owned, non-owned and hired automobile; and
3. Workers' Compensation insurance as required by the Labor Code of the State of California and Employers Liability insurance.
4. Professional Liability Errors and Omissions insurance for professional services.

There shall be no endorsements reducing the scope of coverage required above Unless approved by the City's Risk Manager.

D-2 Minimum Limits of Insurance

Contractor shall maintain limits no less than:

1. Commercial General Liability: \$1,000,000 per occurrence for bodily injury, personal injury and property damage. If Commercial General Liability Insurance or other form with a general aggregate limit is used, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.
2. Automobile Liability: \$1,000,000 combined single limit per accident for bodily injury and property damage.
3. Workers' Compensation and Employers Liability: Workers' Compensation limits as required by the Labor Code of the State of California and Employers Liability limits of \$1,000,000 per accident.
4. Professional Liability Errors and Omissions: \$1,000,000 per occurrence/aggregate.

D-3 Deductibles and Self-Insured Retentions

Any deductibles or self-insured retentions must be declared to, and approved by, the City. At the option of the City, either: the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the City, its officials, employees, agents and contractors; or the Contractor shall procure a bond guaranteeing payment of losses and related investigations, claim administration and defense expenses in an amount specified by the City.

D-4 Other Insurance Provisions

The policies are to contain, or be endorsed to contain, the following provisions:

1. General Liability and Automobile Liability Coverages

- a. The City, its officials, employees, agents and contractors are to be covered as additional insureds as respects: liability arising out of activities performed by, or on behalf of, the Contractor; products and completed operations of the Contractor; premises owned, leased or used by the Contractor; or automobiles owned, leased, hired or borrowed by the Contractor. The coverage shall contain no special limitations on the scope of protection afforded to the City, its officials, employees, agents and contractors.
- b. The Contractor's insurance coverage shall be primary insurance as respects the City, its officials, employees, agents and contractors. Any insurance or self-insurance maintained by the City, its officials, employees, agents or contractors shall be excess of the contractor's insurance and shall not contribute with it.
- c. Any failure to comply with reporting provisions of the policies shall not affect coverage provided to the City, its officials, employees, agents, or contractors.
- d. Coverage shall state that the Contractor's insurance shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of the insurer's liability.
- e. Coverage shall contain a waiver of subrogation in favor of the City, its officials, employees, agents and contractors.

2. Workers' Compensation and Employers' Liability

Coverage shall be endorsed to state carrier waives its rights of subrogation against the City, its officials, agents and contractors

3. All Coverages

Each insurance policy required by this clause shall be endorsed to state that coverage shall not be suspended, voided, canceled, reduced in coverage or in limits except after thirty (30) days' prior written notice has been given to the City; except that ten (10) days' prior written notice shall apply in the event of cancellation for non-payment of premium.

D-5 Acceptability of Insurance

Insurance is to be placed with insurers acceptable to the City's Risk Manager.

D-6 Verification of Coverage

Contractor shall furnish the City with certificates of insurance and with original endorsements affecting coverage required by this clause. The certificates and endorsements for each insurance policy are to be signed by a person authorized by that insurer to bind coverage on its behalf.

Copies of all the required ENDORSEMENTS shall be attached to the CERTIFICATE OF INSURANCE which shall be provided by the Contractor's insurance company as evidence of the stipulated coverages. This proof of insurance shall then be mailed to:, **CITY OF SAN JOSE – HUMAN RESOURCES, Risk Management, 200 East Santa Clara Street 2nd Floor Wing, San Jose, CA 95113-1905**

D-7 Subcontractors

Contractors shall include all subcontractors as insureds under its policies or shall obtain separate certificates and endorsements for each subcontractor

EXHIBIT D
SOFTWARE LICENSE AGREEMENT

1. Scheidt & Bachmann (hereinafter “S&B”) grants to City of San Jose (hereinafter “Customer” or “City”) an irrevocable, perpetual, nonexclusive, non-transferable (other than to Affiliate), fully paid – up right and license to use, display, copy and maintain the enterVo Application Software (Standard Software) limited to Customer’s internal business purposes, which includes the right to make backup copies and to use the Software at unlimited workplaces.
2. The use of the Software is exclusively limited to the operation of the System at the parking facilities of Customer to which S&B delivered the Software and which are subject of the Agreement for the Upgrade and Expansion of a Parking Revenue Control System (“Agreement”).
3. All original software, patent, copyright and/or intellectual or industrial property rights shall remain the sole property of S&B.
4. This rights granted under this License authorize Customer to :
 - a. load the Software on Scheidt & Bachmann Hardware,
 - b. transfer or store on other City owned devices.,,
 - c. receive copies of the Software from S&B on media appropriate to the computer system
 - d. copy the Software to ensure normal computer system operation and transmit the same in the computer system for processing and use by an unlimited number of users of the City under the Agreement;
 - e. make copies of the Software in machine-readable form for emergency back-up, fall-back and archiving copies of the documentation for its own use only;
 - f. transfer the software from one unit to another unit within the parking management system at the City of San Jose.
5. Customer is not permitted to:
 - a. to use the Software for any purpose other than as provided above;
 - b. to remove or modify any program markings or any notice of our proprietary rights;
 - c. translate, work out, combine or otherwise change it;
 - d. cause or permit reverse engineering, disassembly or decompilation of the programs; regulations due to mandatory law will be unaffected by this requirement
6. The right of use of Application Software which has been granted to Customer may not be transferred to third parties without S&B’s written authorization.
7. S&B reserves the right to reject disclosure of software development information as far as it is a business secret. If disclosure becomes necessary, the content of disclosure shall be determined by the parties in further negotiations or by order of a court.
8. S&B shall provide City with its standard software documentation.
9. Customer assumes all obligations and responsibilities for meeting the terms and conditions Third Party Software Licenses included in equipment provided by S&B. (i.e. Microsoft Windows)
10. Either Party shall promptly inform the other Party of any claim, action or suit against the Parties of any claim that the use of the software constitutes an infringement of any patent, copyright and/or any other intellectual or industrial property right of any third party.
11. Contractor Software Warranty
Unless otherwise stated in the Software License Agreement, for one (1) year from the date of Final System Acceptance. Contractor warrants the Contractor Software in accordance with the terms of the Software License Agreement and the provisions of this Section applicable to the Contractor Software.

12. Warranty Against Infringement

Contractor warrants that the Software does not violate or infringe upon any patent, copyright, trade secret, or other proprietary rights of any other person or entity. Contractor agrees to hold the City harmless from any liability and to defend and indemnify the City, at Contractor's sole expense, in the event that a claim is filed or a suit is brought against City or any of its officers, employees, or authorized agents, for the use of the Software due to a patent or copyright infringement by the Software. Contractor further agrees that if the Software is found to be infringing, Contractor will, within one (1) year: (1) Modify the Software, at Contractor's expense, so it becomes non-infringing, or (2) Replace the infringing Software with equal non-infringing Software, at Contractor's expense, or (3) Procure, at Contractor's expense, the necessary licenses for the City to continue using the Software.

13. Operability

Contractor warrants that the Software does not contain any timers, counters, or preprogrammed devices that will cause the Software to become erased, inoperable, or incapable of processing in the manner as documented in the contract documents specified.

14. Upgrades

Contractor agrees to collaborate with the City to maintain the Software as operational on all compatible upgrades of the hardware product line and operations system used by City and specified in the License Agreement. A migration to a new operating system (MS Vista or beyond) or hardware platform may require both a significant time and financial component to be negotiated with the City.

15. Disabling Devices

Contractor warrants that the APPLICATION SOFTWARE and CUSTOM SOFTWARE delivered under this Agreement has been reviewed and does not contain any "back door," "time bomb," "Trojan horse," "worm," "drop dead device," "virus," or other computer software routines or hardware components designed to (i) permit access or use of either the System or City's computer systems by Contractor or a third party not authorized by this Agreement, (ii) disable, damage or erase the System or data, or (iii) perform any other such actions. Further, Contractor warrants that the System and the design thereof shall not contain preprogrammed preventative routines or similar devices which prevent City from exercising the rights set forth in this Agreement or from utilizing the System for the purposes for which it was designed.

16. New Media. Media upon which the Software is delivered to City:

- a. Shall be new and shall be free from defects in manufacture and materials,
- b. Shall be manufactured in a good and workmanlike manner using a skilled staff fully qualified to perform their respective duties.
- c. Shall, during the Warranty Period, function properly under ordinary use and operate in conformance with the Specifications.
- d. In the event that media on which any SOFTWARE APPLICATION, CUSTOM SOFTWARE, or THIRD PARTY APPLICATION SOFTWARE is delivered is defective and cannot be read or utilized for its intended purpose by Contractor supplied or approved equipment, Contractor shall replace the defective media as soon as possible. Any delays occasioned by the failure of new media shall not be considered excusable delay.

17. Specifications

The APPLICATIONS SOFTWARE AND CUSTOM SOFTWARE shall, during the Warranty Period, function properly under ordinary use and operate in conformance with its Specifications and Documentation. During the Warranty Period, Contractor will provide warranty Service to City at no additional cost and will include all Services or replacement

products or product media necessary to enable Contractor to comply with the foregoing warranty. Contractor shall pass through to City any manufacturers' warranties which Contractor receives on the System and, at City's request, Contractor shall enforce such warranties on City's behalf.

18. Warranty Claims

Before the expiration of the warranty period, City must notify Contractor in writing if Equipment or Contractor Software does not conform to these warranties. Upon receipt of such notice, Contractor will investigate the warranty claim. If this investigation confirms a valid warranty claim, Contractor will (at its option and at no additional charge to City) repair the defective Equipment or Contractor Software, replace it with the same or equivalent product, or refund the price of the defective Equipment or Contractor Software. Such action will be the full extent of Contractor's liability hereunder. Repaired or replaced product is warranted for the balance of the original applicable warranty period. All replaced products or parts will become the property of Contractor.

Scheidt & Bachmann USA, Inc.
a Delaware Corporation

City of San Jose
a municipal corporation

By: 
Name: John C. Macdonald
Title: Treasurer
Date: 1/21/2009

By: _____
Name: _____
Title: _____
Date: _____

EXHIBIT F



LABOR COMPLIANCE ADDENDUM

AGREEMENT TITLE:	2ND/SAN CARLOS GARAGE AND PCI UPGRADE PROJECT
CONTRACTOR Name and Address:	Scheidt and Bachman USA Inc. 31 North Avenue Burlington MA 01803

By executing this Addendum, Contractor acknowledges and agrees that the work performed pursuant to the above referenced Agreement or Service Order is subject to all applicable provisions.

Payment of Minimum Compensation to Employees. Contractor shall be obligated to pay not less than the General Prevailing Wage Rate and/or Living Wage Rate as indicated in the attached Exhibit(s) titled **Work Classification and/or Living Wage Determination.**

A. Prevailing Wage Requirements. California Labor Code and/ or Resolutions of the San Jose City Council require the payment of not less than the general prevailing rate of per diem wages and rates for holiday and overtime and adherence to all labor standards and regulations. The General Prevailing Wage Rates may be adjusted throughout the term of this Agreement. Notwithstanding any other provision of this Agreement, Contractor shall not be entitled to any adjustment in compensation rates in the event there are adjustments to the General Prevailing Wage Rates.

B. Living Wage Requirements. Any person employed by Contractor or subcontractor or City financial recipient or any sub recipient whose compensation is attributable to the City’s financial assistance, who meets the following requirements is considered a covered employee. The employee: 1) is not a person who provides volunteer services, that are uncompensated except for reimbursement of expenses such as meals, parking or transportation; 2) spends at least half of his or her time on work for the City [4 hours a day or 20 hours a week]; 3) is at least eighteen (18) years of age; and 4) is not in training for the period of training specified under training standards approved by the City.

C. Reports. Contractor shall file a completed and executed copy of this Addendum with the Department of Finance. Upon award the Department of Finance shall provide the contractor with compliance documents to be completed and returned (with supporting documentation) to the Office of Equality Assurance. **These documents must be returned within 10 days of receipt.** Contractor shall not perform on site work on this contract until labor compliance documents are filed. Contractor shall also report additional information, including certified payrolls, as requested by Director of Equality Assurance to assure adherence to the Policy.

D. Coexistence with Any Other Employee Rights. These provisions shall not be construed to limit an employee's ability to bring any legal action for violation of any rights of the employee.

E. Audit Rights. All records or documents required to be kept pursuant to this Agreement to verify compliance with the Wage Requirement shall be made available for audit at no cost to City, at any time during regular business hours, upon written request by the City Attorney, City Auditor, City Manager, or a designated representative of any of these officers. Copies of such records or documents shall be provided to City for audit at City Hall when it is practical to do so. Otherwise, unless an alternative is mutually agreed upon, the records or documents shall be available at Contractor's address indicated for receipt of notices in this Contract.

F. Enforcement.

1. **General.** Contractor acknowledges it has read and understands that, pursuant to the terms and conditions of this Agreement, it is required to comply with the Wage Requirement and to submit certain documentation to the City establishing its compliance with such requirement.

("Documentation Provision.") Contractor further acknowledges the City has determined that the Wage Requirement promotes each of the following (collectively "Goals"):

- a. It protects City job opportunities and stimulates the City's economy by reducing the incentive to recruit and pay a substandard wage to labor from distant, cheap-labor areas.
- b. It benefits the public through the superior efficiency of well-paid employees, whereas the payment of inadequate compensation tends to negatively affect the quality of services to the City by fostering high turnover and instability in the workplace.
- c. Paying workers a wage that enables them not to live in poverty is beneficial to the health and welfare of all citizens of San Jose because it increases the ability of such workers to attain sustenance, decreases the amount of poverty and reduces the amount of taxpayer funded social services in San Jose.
- d. It increases competition by promoting a more level playing field among contractors with regard to the wages paid to workers.

2. **Remedies for Contractor's Breach of Prevailing Wage/Living Wage Provisions.**

a. **WITHHOLDING OF PAYMENT:** Contractor agrees that the Documentation Provision is critical to the City's ability to monitor Contractor's compliance with the Wage Requirement and to ultimately achieve the Goals. Contractor further agrees its breach of the Documentation Provision results in the need for additional enforcement action to verify compliance with the Wage Requirement. In light of the critical importance of the Documentation Provision, the City and Contractor agree that Contractor's compliance with this Provision, as well as the Wage Requirement, is an express condition of City's obligation to make each payment due to the Contractor pursuant to this Agreement. **THE CITY IS NOT OBLIGATED TO MAKE ANY PAYMENT DUE THE CONTRACTOR UNTIL CONTRACTOR HAS PERFORMED ALL OF ITS OBLIGATIONS UNDER THESE PROVISIONS. THIS PROVISION MEANS THAT CITY CAN WITHHOLD ALL OR PART OF A PAYMENT TO CONTRACTOR UNTIL ALL REQUIRED DOCUMENTATION IS SUBMITTED.** Any payment by the City despite Contractor's failure to fully perform its obligations under these provisions shall not be deemed to be a waiver of any other term or condition contained in this Agreement or a waiver of the right to withhold payment for any subsequent breach of the Wage Requirement or the Documentation Provision.

b. **RESTITUTION:** Require the employer to pay any amounts underpaid in violation of the required payments and City's administrative costs and liquidated damages and, in the case of financial assistance, to refund any sums disbursed by the City.

c. **SUSPENSION OR TERMINATION:** Suspend and/or terminate Agreement for cause;

- d. **DEBARMENT:** Debar Contractor or subcontractor from future City contracts and/or deem the recipient ineligible for future financial assistance.
- e. **LIQUIDATED DAMAGES FOR BREACH OF WAGE PROVISION:** Contractor agrees its breach of the Wage Requirement would cause the City damage by undermining the Goals, and City's damage would not be remedied by Contractor's payment of restitution to the workers who were paid a substandard wage. Contractor further agrees that such damage would increase the greater the number of employees not paid the applicable prevailing wage and the longer the amount of time over which such wages were not paid. The City and Contractor mutually agree that making a precise determination of the amount of City's damages as a result of Contractor's breach of the Wage Requirement would be impracticable and/or extremely difficult. **THEREFORE, THE PARTIES AGREE THAT, IN THE EVENT OF SUCH A BREACH, CONTRACTOR SHALL PAY TO THE CITY AS LIQUIDATED DAMAGES THE SUM OF THREE (3) TIMES THE DIFFERENCE BETWEEN THE ACTUAL AMOUNT OF WAGES PAID AND THE AMOUNT OF WAGES THAT SHOULD HAVE BEEN PAID.**

City

Contractor

By _____
Name: Mark Giovannetti
Title: Purchasing Officer
Date: _____

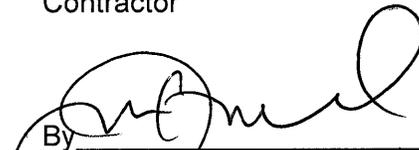
By  _____
Name: John C. MacDonato
Title: Treasurer
Date: 12/2/2009

Exhibit G Project Schedule

SJO-2nd San Carlos_ Revised_1_6_09

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
0	SJO-2nd San Carlos_ Revised_1_6_09	502 days?	Tue 9/2/08	Fri 8/27/10		
1	Contract Phase	105.13 days?	Tue 9/2/08	Tue 2/3/09		
2	Contract Negotiations	5 days	Tue 9/2/08	Mon 9/8/08		J MacDonald[25%],C
3	Contract Executed by S & B	0.13 days?	Wed 9/10/08	Wed 9/10/08	2FS+1 day	J MacDonald
4	Contract Executed by Customer and Received by S & B	0.13 days?	Tue 2/3/09	Tue 2/3/09	3FS+14 days	Customer
5	Production and Purchasing	74 days?	Mon 2/23/09	Fri 6/5/09		
6	Bill of Material Preparation	2.5 days	Mon 2/23/09	Wed 2/25/09	3FS+3 days	M Loudenback[20%]
7	Order Confirmation Received from GmbH	0.13 days?	Wed 3/11/09	Wed 3/11/09	6FS+10 days	M Loudenback
8	Purchase Order Creation for GmbH	0.38 days?	Thu 3/12/09	Thu 3/12/09	7FS+1 day	M Loudenback
9	Third Party Equipment Ordered(List each individually)	0.38 days	Mon 3/2/09	Mon 3/2/09	6FS+3 days	M Loudenback
10	Third Party Equipment Received(List each individually)	0.13 days?	Mon 3/23/09	Mon 3/23/09	9FS+15 days	J O Neil
11	GmbH Equipment Produced, Shipped and Received in Burlington	60 days?	Fri 3/13/09	Fri 6/5/09	8	J O Neil[0%]
12	Customer Obligations	0.13 days?	Thu 3/5/09	Thu 3/5/09		
13	Provide Rate Structure	0.13 days?	Thu 3/5/09	Thu 3/5/09	4FS+21 days	Customer
14	Provide DSL Line for Credit Card Server	0.13 days?	Thu 3/5/09	Thu 3/5/09	4FS+21 days	Customer
15	Provide Credit Card Clearing House Info	0.13 days?	Thu 3/5/09	Thu 3/5/09	4FS+21 days	Customer
16	Subcontractor Contract	1.38 days?	Tue 2/3/09	Wed 2/4/09		
17	Subcontract Customized	1.38 days?	Tue 2/3/09	Wed 2/4/09		
18	Scope of Work prepared by PM	0 days	Tue 2/3/09	Tue 2/3/09	4	K Austin
19	Price Proposal Fine Tuned by Subcontract and Presented to S & B	0.13 days?	Wed 2/4/09	Wed 2/4/09	18FS+1 day	Contractor
20	Subcontract customized for this project	0 days	Wed 2/4/09	Wed 2/4/09	19	J MacDonald
21	Subcontract Executed by S & B	0.13 days?	Wed 2/4/09	Wed 2/4/09	20	J MacDonald
22	Subcontract Executed and Returned to S & B with Insurance Cert/Bonds	0.13 days?	Wed 2/4/09	Wed 2/4/09	21	Contractor
23	Factory Acceptance Test	109.88 days?	Tue 2/3/09	Thu 7/9/09		
24	Preparation	67.5 days?	Thu 3/26/09	Tue 6/30/09		
25	Layout and Equipment List provided to Logistics by PM	0.5 days?	Thu 3/26/09	Thu 3/26/09	6FS+21 days,13	Project Manager
26	Equipment Collected and Delivered to FAT Room	5 days	Mon 6/8/09	Fri 6/12/09	10,11,25FS+3 day	J O Neil[20%]
27	Equipment unpacked, arranged, wired and fully setup(incl potential BNA install)	2 days	Mon 6/15/09	Tue 6/16/09	26	Technician[250%]
28	Equipment configured	9 days	Wed 6/17/09	Mon 6/29/09	27,31	A Sterckx[56%],Tech
29	Internal Testing	1 day	Tue 6/30/09	Tue 6/30/09	28	Project Manager[200%
30	Internal Factory Acceptance Test	109.88 days?	Tue 2/3/09	Thu 7/9/09		
31	Testing Documentation	7 days?	Tue 2/3/09	Thu 2/12/09	4	Project Manager[71%
32	Testing Period	0 days	Tue 7/7/09	Tue 7/7/09	31,29FS+4 days	Customer[125%],Proj
33	Adjustments as a result of test with customer	0 days	Tue 7/7/09	Tue 7/7/09	32	A Sterckx
34	Unwire, crate and ship	2 days	Wed 7/8/09	Thu 7/9/09	33	Technician[200%]
35	Installation	385.5 days?	Thu 2/19/09	Fri 8/27/10		
36	Subcontractor Prerequisites by Garage	5 days	Thu 2/19/09	Thu 2/26/09		
37	Run Conduit, Fiber, Power and misc items	5 days	Thu 2/19/09	Thu 2/26/09	22FS+10 days	Contractor[3%]
38	Head End Installation	1 day?	Fri 7/17/09	Fri 7/17/09		
39	Mount, Wire and Power up all head end equipment	1 day?	Fri 7/17/09	Fri 7/17/09	34FS+5 days,37	Hotline
40	On-site Installation	11 days?	Fri 7/17/09	Fri 7/31/09		
41	Install Entry Lanes	1 day	Fri 7/17/09	Fri 7/17/09	39SS,34FS+5 day	Technician[400%]
42	Install Exit Lanes	2 days	Mon 7/20/09	Tue 7/21/09	41	Technician[200%]
43	Install POFs	1 day	Wed 7/22/09	Wed 7/22/09	42	Technician[400%]
44	Testing of Lane Equipment -SAT with the City	1 day?	Thu 7/23/09	Thu 7/23/09	41,42,43	Customer,Project Man
45	Deviation adjustments from SAT	5 days	Fri 7/24/09	Thu 7/30/09	44	
46	Retest Deviations from SAT	1 day?	Fri 7/31/09	Fri 7/31/09	45	
47	Final Acceptance	20 days	Fri 7/31/09	Sun 8/30/09		
48	Operational Testing Period- 30 Calendar Days	30 edays	Fri 7/31/09	Sun 8/30/09	46	
49	Warranty	251 days?	Mon 8/31/09	Fri 8/27/10		
50	Start of Warranty period	1 day?	Mon 8/31/09	Mon 8/31/09	48	
51	1st PM Cycle	3 days	Thu 10/1/09	Mon 10/5/09	48FS+22 days	Technician

Exhibit G Project Schedule

SJO-2nd San Carlos_ Revised_1_6_09							
ID		Task Name	Duration	Start	Finish	Predecessors	Resource Names
52		2nd PM Cycle	3 days?	Tue 1/5/10	Thu 1/7/10	51FS+60 days	Technician
53		3rd PM Cycle	3 days?	Mon 4/5/10	Wed 4/7/10	52FS+60 days	Technician
54		4th PM Cycle	3 days?	Fri 7/2/10	Tue 7/6/10	53FS+60 days	Technician
55		Remaining Warranty period	38 days	Wed 7/7/10	Fri 8/27/10	54	