

Solicitation RFQ 15414

Mobile Solutions Application



City of San Jose

Bid RFQ 15414

Mobile Solutions Application

Bid Number RFQ 15414
Bid Title Mobile Solutions Application

Bid Start Date Mar 29, 2012 6:21:09 PM PDT
Bid End Date Apr 18, 2012 5:00:00 PM PDT
Question & Answer End Date Apr 9, 2012 1:00:00 PM PDT

Bid Contact Celia Alvares
 Buyer II
 Finance
 408-535-7048
 celia.alvares@sanjoseca.gov

Contract Duration 1 year
Contract Renewal 3 annual renewals
Prices Good for 1 year

Bid Comments The City of San Jose is seeking quotes from qualified contractors to provide the implementation of a Mobile Solution application that will be integrated to enhance the overall use of the INFOR Enterprise Asset Management (EAM) Computerized Maintenance Management System (CMMS) application in the field at the Norman Y. Mineta San Jose International Airport (SJC Airport) as per the specifications and requirements herein.
 Contractor shall provide the following services:
 1) Project management and coordination
 2) System installation, configuration and integration
 3) System testing and commissioning
 4) System warranty and maintenance
 5) System training for two (2) administrators and twelve (12) users.
REQUIREMENTS:
 1) See Attachments and/or related documents for details.
 2) Please refer to the RFQ Instructions document and any other attached documents.
 Attachments and required information shall be uploaded to your quote response in the following order:
 1) Attachment A - Support & Maintenance
 2) Attachment B - Requirements Matrix
 3) Attachment C - Previous Customer Reference Form
 4) Network Diagram - Include a high-level network diagram of the proposed solution that shows the servers, devices, required connectivity, protocols and security architecture recommended to secure the server and communication with the device, and any variations/options in the architectural configuration
 5) Project Plan - Provide a high level project plan to include milestones with a timeline detailing project completion. Include assumptions of the roles and time commitments of Airport staff and a one page resume of the Project Manager that will be assigned to this project
 6) Training - Submit your firms training program
AWARD BASIS - Non-price determinative:
 The award for this requirement will be a "best value" procurement based on the City's evaluation as per the following criteria and weights:
 Technical Capabilities: 40 %
 Experience: 30 %
 Cost: 20 %
 Local Business Preference: 5 %
 Small Business Preference: 5 %
 Total 100 %
ADDITIONAL REQUIREMENTS: The following additional requirements apply to the successful contractor (see attached documents) and must be provided within five calendar days of

notification of award:**1) Insurance****QUOTE SUBMISSION:**

1) All quote responses must be done online through BidSync, including electronic attachments if applicable. The City will no longer accept hardcopy quotes.

2) All line items must be priced or clearly show "No Charge" or "included" not left blank or zero.

PRICING:

1) All pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/ administrative costs required to complete each task(labor rates must be all inclusive).

2) Consideration for local and small business preference will be applied to the total base bid by the City as applicable. Proposers must complete the LBE/SBE form to be eligible for this preference.

3) Only prices that appear on this RFQ will be considered. No other pages with prices and no attached price lists will be considered.

4) Cost shall be scored based on the Total Base Price.

PRICE ADJUSTMENTS: In the event the City elects to exercise its option for annual renewals, price adjustments will be considered by the City if the vendor demonstrates to the satisfaction of the City that price increase is justified. Any increase shall not exceed 3% annually.

Added on Apr 3, 2012:

~

Changes made on Apr 3, 2012 2:46:26 PM PDT

New Documents

Airport Security Standards.pdf

Item Response Form

Item	RFQ 15414--01-01 - RFQ 15414 Mobile Solutions Application Pricing: Business Server License Fee
Lot Description	1. Pricing must be for total cost of project for which you are to be considered. 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/ administrative costs required to complete each task (labor rates must be all inclusive). 3. Cost proposals shall be scored based on Total Base Price.
Quantity	1 each
Unit Price	
Delivery Location	City of San Jose <u>No Location Specified</u>
	Qty 1
Description	
Pricing to include three Desktop Administrator seats (1)System and (2) Business Administrators	

Item	RFQ 15414--01-02 - RFQ 15414 Mobile Solutions Application Pricing: Mobile Smart Client License Fee
Lot Description	1. Pricing must be for total cost of project for which you are to be considered. 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/ administrative costs required to complete each task (labor rates must be all inclusive). 3. Cost proposals shall be scored based on Total Base Price.
Quantity	12 each
Unit Price	

Delivery Location **City of San Jose**
No Location Specified

Qty 12

Description
 Annual Term

Item **RFQ 15414--01-03 - RFQ 15414 Mobile Solutions Application Pricing: Maintenance & Support**

Lot Description **1. Pricing must be for total cost of project for which you are to be considered.
 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/administrative costs required to complete each task (labor rates must be all inclusive).
 3. Cost proposals shall be scored based on Total Base Price.**

Quantity **1 each**

Unit Price

Delivery Location **City of San Jose**
No Location Specified

Qty 1

Description
 1 year

Item **RFQ 15414--01-04 - RFQ 15414 Mobile Solutions Application Pricing: Server Software (Install & Configure)**

Lot Description **1. Pricing must be for total cost of project for which you are to be considered.
 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/administrative costs required to complete each task (labor rates must be all inclusive).
 3. Cost proposals shall be scored based on Total Base Price.**

Quantity **1 lot**

Unit Price

Delivery Location **City of San Jose**
No Location Specified

Qty 1

Description
 to include all labor as well as any additional costs required to complete each task (labor rates must be all inclusive)

Item **RFQ 15414--01-05 - RFQ 15414 Mobile Solutions Application Pricing: Client Software (install & configure)**

Lot Description **1. Pricing must be for total cost of project for which you are to be considered.
 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/administrative costs required to complete each task (labor rates must be all inclusive).
 3. Cost proposals shall be scored based on Total Base Price.**

Quantity **1 lot**

Unit Price

Delivery Location **City of San Jose**
No Location Specified

Qty 1

Description

MobileFrame client software to include all labor as well as any additional costs required to complete each task (labor rates must be all inclusive)

Item	RFQ 15414--01-06 - RFQ 15414 Mobile Solutions Application Pricing: Advance Training for Administrators
Lot Description	1. Pricing must be for total cost of project for which you are to be considered. 2. All Pricing is "firm fixed" for a one year period and must account for all costs, include all labor as well as any additional reimbursable expenses/administrative costs required to complete each task (labor rates must be all inclusive). 3. Cost proposals shall be scored based on Total Base Price.
Quantity	2 each
Unit Price	
Delivery Location	City of San Jose <u>No Location Specified</u>
	Qty 2
Description	.

REQUEST FOR QUOTATION (RFQ) – INSTRUCTIONS AND GENERAL PROVISIONS

1 SUBMITTING THE QUOTATION

Electronic Submission. The City of San José (“CITY”) requires that quotes be submitted electronically on the BidSync System. Bidders must register with BidSync and complete the required Bidder registration and the supplemental Bidder qualifications that are specific to the CITY. The direct link to BidSync is www.bidsync.com or you may register via the CITY’s internet Bidline at www.sanjoseca.gov. All bids are secure and may not be accessed until the date and time indicated in this RFQ. Bidders may modify or withdraw any quote prior to the bid close. It is the sole responsibility of the Bidder to ensure its quote is submitted before the closing date and time and the CITY is not responsible for any late or incomplete submissions due to any technical issues that may be encountered on the website. **There is no cost to the Bidder to register, receive or submit electronic quotes using BidSync.**

2 QUOTATION PREPARATION

- (a) The time stated as the deadline for response submittal is critical and must be adhered to as specified.
- (b) Unless specifically stated as “no substitutions allowed”, whenever an item is described by using a brand/trade name of a manufacturer and/or model number, it is intended that the words, “or equal” apply. “Or equal” means any other brand that is equal or equivalent to the named brand in meeting the specific operational, design, performance, maintenance, quality, and reliability requirements of the CITY as determined in the CITY’S sole discretion. All quotes offering an equivalent product must include complete manufacturer’s descriptive literature for that product. The CITY reserves the right to test and evaluate the product. At the Bidder’s expense, the Bidder bears sole responsibility for providing any information, test data or document required by the CITY to fully evaluate the acceptability of the “or equal.” At the Bidder’s expense, this full evaluation may require independent testing, including destructive testing, at qualified test facilities. If the Bidder lists a brand/trade name and/or catalog number in the quote, CITY will assume the item meets the specifications unless the quote clearly states otherwise and describes specifically how it differs from the item specified. All products are to be of new, unused condition, unless otherwise requested in this solicitation.
- (c) By submitting the quotation The Bidder’s submitted quotation constitutes the Bidder’s offer to provide the CITY the item(s) specified at the quoted price(s) on the terms and conditions set forth in the complete RFQ solicitation package including this document.
- (d) The CITY may designate incomplete quotes as non-responsive

3 LABOR COMPLIANCE

If Living and/or Prevailing Wage is required for this procurement, the Bidder shall be required to sign and submit a hardcopy of the Labor Compliance Addendum within five calendar days after notification of award. The Addendum and all wage requirements will be included with each RFQ as applicable.

4 INSURANCE REQUIREMENTS

CITY's insurance requirements are included with this solicitation document. The Bidder recommended for award must provide proof of insurance within five calendar days after notice of award.

5 BOND REQUIREMENTS

If a Payment Bond is required for this procurement, the Bidder recommended for award must submit a Payment Bond executed by a surety naming the City of San Jose as beneficiary for 100% of the contract price within ten calendar days after notice of award.

6 LOCAL AND SMALL BUSINESS PREFERENCE

- (a) It is the policy of the City of San José to encourage local and small business activity by providing preferences in the award of contracts in accordance with San Jose Municipal Code Section 4.12.320.
- (b) To respond to this solicitation, Bidders must register on-line with BidSync and complete the "Qualifications for this Agency" under the "Steps for Placing a Bid" section of the on-line solicitation. In order to claim the Local and/or Small Business Preference, Bidders must complete the required on-line information and check the appropriate check-boxes for Local and/or Small Business Preference.
- (c) If the basis of award is price determinative (awarded to the low bidder) then the amount of the preference shall be 2.5% of cost for Local and an additional 2.5% of cost for Small.
- (d) If the basis of award is points determinative ("best value") then the amount of the preference shall be 5% of total points for Local and an additional 5% of total points for Small.

7 RFQ QUESTIONS AND ANSWERS

- (a) All questions regarding the RFQ (including but not limited to questions about the products and/or services to be procured) are to be addressed to the responsible Procurement Contact utilizing the Question and Answer facilities contained on the BidSync Website for each RFQ.
- (b) Answers to questions submitted through BidSync will be answered on BidSync, and shall be considered addenda to the RFQ.
- (c) Oral interpretations or clarifications will be without legal effect.
- (d) Bidders shall not contact or ask questions of any other CITY employee or person involved with the development of the specifications or requirements of the RFQ. Failure to observe this requirement shall render a quotation submitted as non-responsive.

8 RFQ AMENDMENTS

All addenda and notices related to this procurement will be posted by CITY on BidSync. In the event this RFQ is obtained through any means other than BidSync, CITY will not be responsible for the completeness, accuracy, or timeliness of the final RFQ, as received by the Bidder.

9 AWARD OF CONTRACT

- (a) Bidders will receive a Pre-Award Notification (also referred to as a "Pre-Award Tabulation Report" or "Bid Tabulation Report") via BidSync. At such time, the results of the RFQ process (including Bidders' submitted quotations) may be publicly reviewed and will be made available on Bidsync.
- (b) The Pre-Award Notification starts the protest process as described in Section 10(b) below.
- (c) The recommended winning Bidder shall have five calendar days from the date of the Pre-Award Notification to provide verification of insurance, five calendar days to complete and submit the Labor Compliance Addendum, if required, and ten calendar days to submit the Payment Bond, if required. If this documentation is not received within the specified time, CITY may declare the recommended winning Bidder's quote non-responsive and award the contract to the second low bidder or second most advantageous Bidder.
- (d) After receipt of all required documentation, CITY will issue a Purchase Order or Agreement for the required products and/or services. Bidder shall not provide any service, ship product, or invoice CITY until such time that a properly executed Purchase Order or Contract has been issued by CITY. Failure to do so may result in return of product(s) at the Bidder's expense or non-payment for services provided.
- (e) The CITY may accept all or part of the quote, or reject any or all quotes.
- (f) Estimated quantities are for quoting purposes only, and not to be interpreted as a guarantee to purchase any amount.
- (g) Contracts may be awarded to multiple Bidders if CITY determines it would be in its best interest.
- (h) For quotations with renewals, all renewals shall be considered as options to renew and will be exercised at the sole discretion of the CITY.

10 OBJECTIONS AND PROTESTS

- (a) Bidders objecting to the specifications contained in the RFQ must contact the Procurement Contact listed in the RFQ in writing (e-mail is acceptable) as soon as possible by the deadline for questions. Objections must be as specific as possible and identify the item number as well as a description and rationale for the objection.
- (b) If an unsuccessful Bidder wants to dispute the award recommendation, the Bidder must notify the Procurement Contact in writing of the Bidder's intent to submit a protest no later than two business days after the Pre-Award Notification is published. The protesting Bidder will then have five calendar days to submit a formal protest in writing to the Purchasing Officer. Protests must detail the grounds, factual basis and provide all supporting information for the protest. Protests will not be considered for disputes of proposal requirements and specifications, which must be addressed in accordance with Subsection (a) above. Protests will not be considered if the Bidder's notice of intent to protest or formal protest is not received within two business days after the Pre-Award Notification indicating the winning Bidder. The Purchasing Officer or designee will respond to the protesting party, as well as any Bidder who is affected by the protest and/or the protest decision. The decision of the Purchasing Officer or designee shall be final.

- (c) The address for submitting protests is:

City of San Jose
200 East Santa Clara Street, 13th Floor
San Jose, CA 95113
Attn: Purchasing Officer

11 PROTECTED INFORMATION

All material submitted in response to the RFQ becomes the property of CITY. Quotes submitted may be reviewed and evaluated by any persons at the discretion of CITY.

12 ENVIRONMENTALLY PREFERABLE PRODUCTS AND SERVICES

- (a) Bidders are encouraged to offer Energy Star, Green Seal, EcoLogo, or EPEAT certified products. CITY also encourages Bidders to offer products and services that are produced or delivered with minimal use of virgin materials and maximum use of recycled materials and reduce waste, energy usage, water utilization, and toxicity in the manufacture and use of products.
- (b) Bidders are encouraged to offer Energy Star certified products or products that meet FEMP (Federal Energy Management Program) standards for energy consumption. CITY also encourages Bidders to offer products that are produced with recycled materials, where appropriate, unless otherwise requested in this RFQ.

13 CITY BUSINESS TAX

If the Bidder is not currently doing business in San José, the Bidder shall have to pay a CITY Business License Tax prior to any commencement of work. For more information, you may contact the Business Tax Office at (408) 535-7055 to determine costs, or Web Site: <http://www.csjfinance.org/>

ATTACHMENT A
CITY OF SAN JOSE, PURCHASE ORDER STANDARD TERMS AND CONDITIONS

1. **DEFINITIONS:** "City" shall mean the City of San José. "Vendor" shall mean the provider of goods and/or services which are the subject of this purchase order. "Director" shall mean the Director of Finance or Director's authorized designee.
2. **CONTRACT:** This purchase order, which consists of these standard terms and conditions, and any attachments hereto, evidences City's acceptance of Vendor's offer to provide to City the goods and/or services which are the subject of this purchase order and constitutes a binding contract therefore upon the terms and conditions set forth herein without further action or agreement of Vendor. In the event of conflict between these standard terms and conditions and the provisions of any attachment hereto, the provisions of the attachment shall control.
3. **SCHEDULE OF GOODS AND/OR SERVICES; TIME OF PERFORMANCE:** Vendor shall supply those goods and/or services which are specified herein, in accordance with the schedule and during the term which are specified herein. Time is of the essence in this purchase order.
4. **COMPENSATION; SCHEDULE OF PAYMENT:** The compensation to be paid and the method of payment to Vendor for goods and services shall be as set forth herein. Unless otherwise provided herein, payment shall not be due until thirty (30) calendar days after the later to occur of the date performance under this purchase order is completed to the satisfaction of City and the date City receives an acceptable invoice. No payment shall represent a waiver of City's right to inspect for defects. Unless otherwise provided herein, Vendor shall be responsible for all costs and expenses incident to the performance of this purchase order, including without limitation all costs of equipment provided by Vendor, all fees, fines, licenses, bonds or taxes required of or imposed against Vendor, and all other of Vendor's costs of doing business.
5. **CURRENT PRICES OF GOODS:** Vendor represents that prices to be paid by City for goods shall not exceed current prices charged to any other customer of Vendor for items which are the same or substantially similar to the goods, taking into account the quality of the goods, and Vendor will forthwith refund any amounts paid by City in excess of such prices.
6. **DISCOUNT PERIODS:** Payment discount periods shall be calculated from the later of the date this purchase order is completed or the date City receives an acceptable invoice, to the date City's payment is sent.
7. **SALES TAXES:** Vendor shall separately state on all invoices any sales, use or similar taxes imposed by federal or state government applicable to furnishing of the goods and/or services; provided, however where a tax exemption is available, such tax shall be subtracted from the total compensation and identified. Municipalities are exempt from federal excise and transportation taxes, except for the excise tax on gasoline. Exemption certificates will be furnished upon request.
8. **PACKING AND SHIPPING OF GOODS; TITLE AND RISK OF LOSS:** All goods shall be delivered "free on board destination" to the location specified herein, full freight prepaid except for special or expedited orders. Deliveries of goods shall be made without charge for boxing, crating, carting or storage unless otherwise specified, and goods shall be suitably packed to secure lowest transportation costs, and in accordance with the requirements of common carriers, and in such a manner as to assure against damage from weather or transportation. City's order numbers and symbols must be plainly marked on all invoices, packages, bills of lading and shipping orders. Packing lists shall accompany each box or package shipment. City's count or weight shall be final and conclusive on shipments not accompanied by packing lists. Shipments for two or more destinations when so directed by City shall be shipped in separate boxes or containers for each destination at no extra charge.

Title to and risk of loss on all goods shall pass to City only upon delivery by Vendor in the manner specified herein and City's acceptance of such goods.

9. **WARRANTIES:** Vendor warrants that all goods and services shall be delivered or performed free of all liens, claims, security interest or encumbrances, will conform to applicable specifications, drawings, descriptions and samples, and will be merchantable, of good workmanship and material, and free from defect. Unless manufactured or performed pursuant to detailed design furnished by City, Vendor assumes design responsibility, and warrants that all goods and services shall be delivered or performed free of design defect and suitable for the purposes intended by City, and that neither purchase, use or resale, nor delivery or performance thereof shall violate any patent, copyright or similar rights. Vendor's warranties shall run to City and shall not be deemed to be exclusive. City's inspections, approval, acceptance, use of or payment for all or any part of the goods or services shall in no way affect its warranty rights whether or not a breach of warranty had become or should have become evident at the time.
10. **CHANGES:** City shall have the right by written notice to change the extent of the work covered by this purchase order, the time or place of delivery, the method of shipment or packaging, or to suspend work. The only valid change is a change order signed by the Director. Upon receipt of any such notice, Vendor shall promptly make the changes in accordance with the terms of the notice. If any such changes cause an increase or decrease in the cost of or time for performance, an equitable adjustment shall be negotiated promptly and the purchase order modified in writing accordingly. Vendor shall promptly deliver to City, and in any event within ten (10) calendar days after receipt of such notice, a statement showing the effect of any such changes in the cost of or time for performance. Failure of Vendor to submit the statement within the above time limit shall constitute its consent to perform the change without increase in compensation or time for performance.
11. **TERMINATION FOR DEFAULT OR CONVENIENCE:** City may, by written notice to Vendor, terminate this purchase order in whole or from time to time in part for default: (i) if Vendor fails to deliver the goods or to perform the services strictly within the time specified herein, or if no time is specified, within a reasonable time; (ii) if the goods delivered or services performed do not conform to the requirements of this purchase order or if Vendor fails to perform any of the other provisions of this purchase order, or so fails to make progress as to endanger performance of this purchase order in accordance with its terms; or (iii) if the Vendor becomes insolvent. If this purchase order is terminated for default, City, in addition to all other rights afforded by law for Vendor's default, shall have the right to charge Vendor the amount by which the costs of fabricating or procuring the goods or services cancelled from another source exceed the compensation specified herein, and City may set off any such charge against any amounts which may become payable to Vendor under this purchase order or otherwise. City may, by not less than thirty (30) days written notice to Vendor, terminate this purchase order for convenience and without cause. In the event of such termination for convenience, Vendor will be paid for those goods delivered and services performed pursuant to this purchase order to the satisfaction of City up to the date of termination. The Director is empowered to terminate this purchase order on behalf of City.
12. **INDEMNITY: TO THE FULLEST EXTENT PERMITTED BY LAW, VENDOR AGREES TO DEFEND, INDEMNIFY AND HOLD HARMLESS THE CITY, ITS OFFICERS, AGENTS AND EMPLOYEES, AGAINST ANY CLAIM, LOSS OR LIABILITY (COLLECTIVELY, "CLAIMS"), INCLUDING WITHOUT LIMITATION CLAIMS FOR INJURIES OR DEATH TO PERSONS OR DAMAGE TO OR DESTRUCTION OF PROPERTY, CAUSED BY OR RESULTING FROM THE ACTS OR OMISSIONS OF VENDOR, ITS OFFICERS, AGENTS, EMPLOYEES OR SUBCONTRACTORS, IN THE PERFORMANCE OF THIS PURCHASE ORDER, OR THE BREACH BY VENDOR OF ANY OF ITS**

OBLIGATIONS UNDER THIS PURCHASE ORDER.

13. **INSURANCE REQUIREMENTS:** If applicable, Vendor agrees to have and maintain the insurance policies specified herein. All policies, endorsements, certificates and/or binders shall be subject to review and approval by the Risk Manager of the City of San Jose as to form and content. These insurance requirements are subject to amendment or waiver if so approved in writing by the Risk Manager. Vendor agrees to provide City with a copy of applicable certificates and/or endorsements before work commences under this purchase order.
14. **COMPLIANCE WITH THE LAW:** Vendor shall in the performance of this purchase order comply with all applicable laws, ordinances, codes and regulations of the federal, state and local governments.
15. **GOVERNING LAW:** City and Vendor agree that the law governing this purchase order shall be that of the State of California.
16. **VENUE:** In the event that suit shall be brought by either party to this purchase order, the parties agree that venue shall 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 José, California.
17. **ASSIGNMENT OF CONTRACT:** Vendor shall not assign any of the work to be performed under this purchase order nor shall Vendor subcontract for complete or substantially completed goods or major components thereof without the Director's prior written consent. Vendor may assign monies due under this purchase order. City will recognize such assignment, to the extent permitted by law, if City is given proper notice thereof. Any assignment shall be subject to set-off or recoupment for any present or future claim which City may have against Vendor.
18. **WAIVER:** Vendor agrees that City's waiver of any breach or violation of any provision of this purchase order 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 Vendor's performance will not be a waiver of any provision of this purchase order.
19. **INDEPENDENT CONTRACTOR:** It is understood and agreed that Vendor shall act as and be an independent contractor and not an employee, agent, joint venturer, or partner of City. As an independent contractor, Vendor shall obtain no rights to retirement benefits or other benefits which accrue to City's employees, and Vendor hereby expressly waives any claim it may have to any such rights. Both parties acknowledge that Vendor is not an employee for state or federal tax purposes. Vendor shall retain the right to perform services for others during the term of this purchase order.
20. **CONFIDENTIAL INFORMATION:** All data, documents, discussions or other information developed or received by or for Vendor in performance of this purchase order are confidential and not to be disclosed to any person except as authorized by City, or as required by law.
21. **OWNERSHIP OF MATERIALS:** All reports, documents or other materials developed or discovered by Vendor or any other person engaged directly or indirectly by Vendor in performance of this purchase order shall be and remain the property of City without restriction or limitation upon their use.
22. **VENDOR'S BOOKS AND RECORDS:** Vendor shall maintain any and all ledgers, books of account, invoices, vouchers, canceled checks, other records or documents evidencing or relating to charges for services, or expenditures and disbursements charged to City for a minimum period of three (3) years, or for any longer period required by law, for the date of final payment to Vendor pursuant to this purchase order. Vendor shall maintain all documents and records which demonstrate performance under this purchase order for a minimum of three (3) years, or for any period longer required by law, from the date of termination or completion of this purchase order. Any records or documents required to be maintained pursuant to this purchase order shall be made available for inspection or audit, at any time during regular business hours, upon written request by City Attorney, City Auditor, City Manager or a designated representative of any of these officers. Copies of such documents shall be provided 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 Vendor's business City may, by written request by any of the above-named officers, require that custody of the records be given to City and that the records and documents be maintained in City Hall. Access to such records and documents shall be granted to any part authorized by Vendor, Vendor's representatives, or Vendor's successor-in-interest.
23. **NON-DISCRIMINATION:**
 - a. **Prohibition on Discrimination and Preferential Treatment.**
CONTRACTOR shall fully comply with Chapter 4.08 of the San Jose Municipal Code and 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 CITY contracts.
 - b. **Compliance Reports.**
If directed by the Director of Office of Equality Assurance of the CITY, CONTRACTOR shall file, and cause any subcontractor to file, compliance reports with the Director of Office of Equality Assurance. Compliance reports shall be in the form and field at such times as may be designated by the Director of Office of Equality Assurance. Compliance reports shall contain such information and be supported by such data or records as may be requested by the Director of Office of Equality Assurance to determine whether CONTRACTOR or its subcontractor is complying with the nondiscrimination and non-preference provisions of this Agreement and Chapter 4.08 of the Municipal Code.
 - c. **Failure to Comply with Nondiscrimination Provisions.**
If the Director of Office of Equality Assurance determines that the CONTRACTOR has not complied with the nondiscrimination or non-preference provisions of this Agreement, the CITY may terminate or suspend this Agreement, in whole or in part. Failure to comply with these provisions may also subject CONTRACTOR and/or subcontractor to debarment proceedings pursuant to provisions of the San Jose Municipal Code. Failure to comply with these provisions is a violation of Chapter 4.08 of the San Jose Municipal Code and is a misdemeanor.
 - d. **Subcontracts.**
CONTRACTOR shall include provisions a through c above, inclusive, in each subcontract entered into in furtherance of this Agreement so that such provisions are binding upon each of its subcontractors.
 - e. **Waiver of Nondiscrimination Provisions.**
The nondiscrimination provisions of this Agreement may be waived by the Director of Office of Equality Assurance, if the Director of Office of Equality Assurance determines that the CONTRACTOR has its own nondiscrimination requirements or is bound in the performance of this Agreement by the nondiscrimination requirements of another governmental agency, and the nondiscrimination provisions of the CONTRACTOR or other governmental agency are substantially the same as those imposed by the CITY.
24. **GIFTS:** CONTRACTOR represents that it is familiar with the City's prohibition against the acceptance for any gift by a CITY officer or designated employee,

which prohibition is found in Chapter 12.08 of the San Jose Municipal Code. CONTRACTOR agrees not to offer any CITY officer or designated employee any gift prohibited by said Chapter. The offer or giving of any gift prohibited by Chapter 12.08 shall constitute a material breach of this SERVICE ORDER by CONTRACTOR. In addition to any other remedies CITY may have in law or equity, CITY may terminate this SERVICE ORDER for such breach.

25. **CONFLICT OF INTEREST:** CONTRACTOR shall avoid all conflict of interest or appearance of conflict of interest in performance of this SERVICE ORDER. **DISQUALIFICATION OF FORMER EMPLOYEES:** CONTRACTOR is familiar with the provisions relating to the disqualification of former officers and employees of CITY in matters which are connected with former duties or official responsibilities as set forth in Chapter 12.10 of the San Jose Municipal Code ("Revolving Door Ordinance"). CONTRACTOR shall not utilize either directly or indirectly any officer, employee, or agent who would be in violation of the Revolving Door Ordinance.

Supplier Acknowledgement Page

RFQ Number: *RFQ 15414*

RFQ Name: *Mobile Solutions Application*

Electronic Submission: The City of San José (“CITY”) requires that quotes be submitted electronically on the BidSync System. You must complete the required information in this form, and electronically sign the document.

The undersigned supplier hereby certifies that he/she understands the specifications, has read the document in its entirety and that the prices submitted in this quotation have been carefully reviewed and are submitted as correct and final. Supplier further certifies that it is authorized to make this response and agrees that it can and will furnish all products/services meeting the specifications of this Request for Quotation upon which prices are extended at the unit price offered, and upon the City’s Standard Terms and Conditions.

Supplier Name:

Company Address:

Contract Telephone Number:

Contact Email Address:

Electronic Purchase Order: The City has transitioned to an electronic Purchase Order (e-PO) printing and e-mail distribution process. To facilitate this process and in the event of PO award, you must provide the e-mail address that the e-PO should be sent to (if different from above):

PO Email Address:

Name (signature):

Name (print):

Title:

Executed at: (City, State)

Date:

INSURANCE REQUIREMENTS FOR CONTRACTORS

(Standard for Contractors)

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.

A. Minimum Scope of Insurance

Coverage shall be at least as broad as:

1. Insurance Services Office Commercial General Liability coverage ("occurrence" form CG 0001), including products and completed operations, and X, C, U where applicable; and
2. Insurance Services Office form number CA 0001 covering Automobile Liability, code 1 "any auto," or code 2 "owned autos" and endorsement CA 0025. Coverage also to include code 8 "hired autos" and code 9 "non-owned" autos; and
3. Workers' Compensation insurance as required by the Labor Code of the State of California and Employers Liability insurance.

B. Minimum Limits of Insurance

CONTRACTOR shall maintain limits no less than:

1. Commercial General Liability: \$1,000,000 combined single limit per occurrence for bodily injury, personal injury and property damage; and
2. Automobile Liability: \$1,000,000 combined single limit per accident for bodily injury and property damage; and
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.

C. 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. Other Insurance Provisions

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

1. Commercial General Liability and Automobile Liability Coverages

- a. The CITY, its officials, employees, agents and contractors are to be covered as an additional insured 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 in 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.

2. All Coverages

Each insurance policy required by this clause shall be endorsed to state that coverage shall not be suspended, voided, canceled, or reduced in limits except after thirty (30) days' prior written notice has been given to the CITY.

E. Acceptability of Insurers

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

F. 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.

Proof of insurance shall be mailed to the following address or any subsequent address as may be directed in writing by the Risk Manager:

City of San Jose – Human Resources
Risk Management
200 East Santa Clara St. 2nd Floor Wing
San Jose, CA 95113-1905

Phone: 408-535-7063
Fax: 408-286-6492

G. Subcontractors

CONTRACTOR shall include all subcontractors as insured under its policies or shall obtain separate certificates and endorsements for each subcontractor.

City of San José
Request for Contracting Preference for Local and Small Businesses

Suppliers Note: You do not need to complete this form if you are submitting an electronic response to a City solicitation (Request for Quotation, Request for Bid, Request for Proposal) on the BidSync system, completed the City of San José Supplemental Qualifications, and checked the appropriate LBE/SBE check-boxes on the Supplemental Qualifications. Contact BidSync directly at 1-800-990-9339, if you have any questions in completing this information.

You do need to print and complete this form, if you are submitting a paper response to a City solicitation and want to be considered for the preference.

Chapter 4.12 of the San José Municipal Code provides for a preference for Local and Small Businesses in the procurement of contracts for supplies, materials, equipment, services. The amount of the preference depends on whether the vendor qualifies as a Local Business Enterprise* or Small Business Enterprise** and whether price has been chosen as the determinative factor in the selection of the vendor.

In order to be a Local Business Enterprise (LBE) you must have a current San José Business Tax Certificate License and have an office in Santa Clara County with at least one employee.

If you qualify as an LBE you may also qualify as a Small Business Enterprise (SBE) if the total number of employees (*regardless of where they are located*) of your firm is 35 or fewer. With respect to quotes, bids, or proposals submitted by partnerships or joint ventures, the number of employees for purposes of qualifying as a SBE shall be determined by the total number of employees of each of the members of the partnership or joint venture combined.

There are two ways in which the preference can be applied:

1) In solicitations where price is the determinative factor (*i.e. there are no other factors being considered in the selection process*) the preference is in the form of a credit applied to the **dollar value** of the response submitted. For example, a non-local vendor submits a response to a City solicitation of \$200 per item and a LBE submits a response of \$204 per item. The LBE receives a 2.5% credit on the response, which equals approximately \$5 and thus the LBE will win the award because the response is evaluated as if it had been submitted as \$199.

2) In solicitations where there are a variety of factors evaluated to determine which response best meets the City's needs, a qualified LBE will be given 5% and a qualified SBE will be given an additional 5% of the total points in the scoring.

***LOCAL BUSINESS ENTERPRISE (LBE) PREFERENCE**

In order to qualify as an LBE you must provide the following information:

Current San José Business Tax License Number
 (Please enter 0 if you don't have a License Number)

Address of Principal Business Office or Regional, Branch or Satellite Office with at least one employee located in Santa Clara County:

***SMALL BUSINESS ENTERPRISE (SBE) PREFERENCE**

In order to qualify as an SBE you must qualify as an LBE and have 35 or fewer employees. This number is for your **entire** business --NOT just local employees, or employees working in the office address given above.

Please state the number of employees that your Business has:

Based upon the forgoing information I am requesting that the Business named above be given the following preferences (*please check*):

☐ Local Business Enterprise ☐ Small Business Enterprise

I declare under penalty of perjury that the information supplied by me in this form is true and correct.

Executed at: _____, California

Date: _____

Signature _____

Print name _____

RFQ 15414 - Attachment A Scope of Services and Requirements

1. General Information

- 1.1. The Facilities & Engineering (F & E) division of Norman Y Mineta San Jose International is seeking a *Mobile Solution* application that can be integrated to enhance the overall use of the INFOR Enterprise Asset Management (EAM) Computerized Maintenance Management Systems (CMMS) application that is currently utilized at this facility.
- 1.2. The F & E division wishes to increase the usage of INFOR Enterprise Asset Management (EAM), Computerized Maintenance Management Systems (CMMS) through a mobile solution that can provide access either through Wi-Fi, stand-alone or docking station capabilities. The new *Mobile Solution* application will be used by the following SJC Facilities & Engineering groups:
 - 1.2.1. Maintenance Services
 - 1.2.2. Trade Services
 - 1.2.3. ATEM, Carpentry, Locksmith, Electrical, Air Conditioning, Paint
 - 1.2.4. Facilities Administrative Services
 - 1.2.5. Facilities Management
 - 1.2.6. Program Manager – Infor EAM
- 1.3. The application will be maintained by the Facilities & Engineering group with support from Airport Technology Services division in cooperation with the selected bidder.

2. Project Goals and Objectives

- 2.1. The SJC Airport requires an extension of the INFOR Enterprise Asset Management (EAM), Computerized Maintenance Management Systems (CMMS) to allow for remote access for identifying and creating work orders and tracking of assets through the work order and asset management system. The objective of the Facilities & Engineering group to effectively track work orders and assets in an effort to:
 - 2.1.1. Decrease costs
 - 2.1.2. Increase productivity
 - 2.1.3. Improve asset-related decision-making
 - 2.1.4. Improve regulatory compliance
 - 2.1.5. Increase business responsiveness
 - 2.1.6. Lower total cost of ownership
- 2.2. **Streamline work operations** through a combination of business process improvement efforts, as well as the implementation of work management functions in an enterprise asset management system that: Allows for both planned and unplanned activities; easily allow work planners to match job tasks to available resources; complete tracking of all work management tasks; and optimize maintenance schedules and labor utilization.
- 2.3. **Improve customer service delivery** through a combination of developing a well-defined service catalog and documented service level metrics along with technology infrastructure in the CMMS to facilitate greater service levels without adding proportionate levels of human resources.
- 2.4. **The goal of this acquisition** is to fully automate work order and asset management processing. The overall solution must capture information completely and accurately at its earliest possible point of entry to the process, and facilitate its most expedient and secure delivery to its endpoint, INFOR EAM.

3. Mobile Solution Software

- 3.1. The selected *Mobile Solution* application must have the flexibility and conformity to provide services to work within the following environments and the ability to:
 - 3.1.1. Configure for use with supported databases (Microsoft SQL Server or Oracle 10 or 11g)
 - 3.1.2. Configure for use with supported Web server (Microsoft IIS)
 - 3.1.3. Function within or with a Windows CE or Android environment
 - 3.1.4. Deploy in any .NET enabled device
 - 3.1.5. Function either in a connected or disconnected capacity
 - 3.1.6. Allow mobile access for troubleshooting services
 - 3.1.7. Set user preferences independently of other users
 - 3.1.8. Prevent users from downloading unwanted applications such as games
 - 3.1.9. Ability to preset update information through a synchronization process
 - 3.1.10. Ability to assist administrators with the use of an integration tool or wizard
 - 3.1.11. Facilitate the delivery of PDF documents between the database and hand-held device
 - 3.1.12. Provide messaging either in a connected or disconnected mode
- 3.2. Complete documentation of all aspect of the solution shall be provided or accessible to Facilities & Engineering online, in CD format or printed hard copies.

4. Software Requirements

4.1. Stability and Maturity

Selected contractor must be an established business in the mobile applications technology sector with a documented history of providing solutions to government and/or nonprofit organizations.

4.2. Proof of Solution Maturity

The selected solution will have a proven track record of successfully and securely managing confidential data and data transmission for organizations of a similar type and size to the Mineta San Jose International Airport.

4.3. Centralized/ Management

The solution must incorporate user authentication, administration, and access control levels appropriate to be capable of efficiently supporting centralized development and modification.

5. Application Compatibility & Co-existence

The selected solution must be compatible and co-exist with existing third party applications and technologies such that data may be accepted from existing databases or read from barcodes; data must also be exportable in industry standard formats for import to other agency databases without conflicts and ideally provide developers advanced customization and integration capabilities.

6. Browser and Mobile Device View ability

The application must render correctly when browsing with current, most-utilized web browsers and as a scalable version for accessibility on handheld devices.

7. Consistent Operation under Varying Connectivity Conditions

All functions of the Infor EAM CMMS system must operate in a consistent manner, whether an end user or administrator is connected to the system through wireless connection or local wireless infrastructure.

8. Secure Data Collection and Transmission

- 8.1. The Solution must enable collection of data and transmission into the repository, whether real-time through active wireless connectivity or, should connection fail, securely store the data for forwarding upon restoration of connectivity.
- 8.2. Devices must be configured so as to protect data content and access, with short time-outs for non-activity that revert to a locked status and require re-authentication to access application and data thereafter.
- 8.3. The application is expected to be available 24 hours per day, 7 days per week for mobile devices to accommodate up to unlimited submissions per month from airport staff and authorized end users.
- 8.4. The *Mobile Solution* should accommodate either stand-alone security or authentication within its functionality, and be configurable for secure authentication to the repository's directory services.

9. Data Integrity/Reliability

The application's design must be such that input is filtered to mitigate errors. Data fields should have appropriate data formats, masks, edits or filters assigned to allow entry of only appropriate data types, i.e., dates in date fields should be formatted as such and within appropriate ranges. Any capability for data validation and cleansing is advantageous to proposals.

10. Maintenance and Support

Since work requests and/or work orders occur at all hours, the selected bidder must have, at minimum, the following levels of maintenance and support capabilities:

- 10.1. Toll-free telephone support from 7:00 a.m. – 7:00 p.m. Pacific time, daily
- 10.2. 24-hour online support, software and documentation update services for both client and server software
- 10.3. An online knowledge base of common problems and frequently asked questions (FAQ)
- 10.4. Online software and documentation update services for both client and server software
- 10.5. Remote troubleshooting/diagnostics

Attachment B – Requirements Matrix (Technical Requirements)

Code	Requirement Title	Requirement Description	Must Have	Included Y/N	Vendor Response Comments
1.00	Access and Security				
1.01	Industry Standard Security	Adopts industry standard security measures, including protection against Cross-Site Scripting (XSS), Structured Query Language (SQL) injection, and directory traversal attacks.	Y		
1.02	Individual & Group Security	Security must be implemented at both individual and group levels (role based).	Y		
1.03	Remote Access	Authorized users shall be able to log into the system from any computer, anywhere, on any device.	N		
1.04	Cross Browser Functionality	Provides cross browser compatibility for administration and publishing	N		
1.05	Industry Standard Password Encryption	If passwords are stored, they shall be encrypted using current industry standard methods.	Y		
1.06	Export capability	Captured data in industry standard format for sharing with other systems	Y		
1.07	Active Directory Integration	User authentication and authorization can be integrated with Active Directory	Y		
1.08	Analytics	Solution to include a web site analytics tool capable of tracking users' navigation throughout the application.	Y		
1.09	TCP/IP Ports Used	Identify TCP/IP ports to be used and any firewall implications	Y		
1.10	Real Time Fault Reports	Solution to provide capability to report faults to system administrators in real time	Y		
1.11	CSJ and Mineta Intern'l Security standards	Meet the City's security standard relative to information security, data storage and transmission	Y		
1.12	Interface	Application can be installed and accessed using Application Programming Interface (API)	Y		
1.13	Configurability	Application can be configured by the system administrator/owner on-site	Y		
1.14	Synchronization	Capable of docked data synchronization with the server without a desktop ODBC connection	Y		

Code	Requirement Title	Requirement Description	Must Have	Included Y/N	Vendor Response Comments
1.15	Deployment Ability	Can deploy new applications or user updates to handheld devices based on user roles	Y		
1.16	Application Access	Provides full remote control of mobile devices	Y		
1.17	Wifi / VPN Access	Can application provide access and synchronization via VPN over the Airport's Wifi network?	Y		
1.18	Secure data transmission	Does application provide secure data transmission methods (such as SSL, secure FTP, secure http, etc.)?	Y		
1.19	Database platform independence	Is the application easily configurable to integrate with diverse database platforms on the back-end? The Airport's INFOR system is currently on Oracle, but eventually will migrate to SQL server.	Y		
1.20	Integration Methods	For integration with the Airport's Infor system, can the access work with a standard Infor API, or otherwise work using restricted privileges?	Y		
2.00	Content Management				
2.01	Meets World Wide Web Consortium (W3C) Publishing Guidelines	System must be capable of rendering and/or creating content that meets the World Wide Web Consortium (W3C) publishing guidelines: such as, Extensible HyperText Markup Language (xHTML), and Web Accessibility Initiative	Y		
2.02	Capabilities	Can route transactions to the proper users' mobile devices from an administrators desktop	Y		
2.03	Content Types	System must be capable of delivering a variety of content types, including at least: Text, Extensible Markup Language (XML), images, barcodes, and Portable Document Format (PDF)	Y		
2.04	Rendering Flexibility	Content must be capable of being rendered through a variety of channels such as: Wireless Application Protocol (WAP), Extensible Markup Language (XML), and HyperText Markup Language (xHTML)	Y		

Code	Requirement Title	Requirement Description	Must Have	Included Y/N	Vendor Response Comments
2.05	Print Preview	Ability to see forms containing content as it will appear before it is generated/printed	Y		
2.06	Meta Data Maintenance	System must support the creation and maintenance of meta data.	Y		
2.07	Graphical or Textual Functionality	The resulting web sites must function equally well in either graphical or text-only mode.	Y		
2.08	Templates & Style Sheets	Ability to create and use different templates and style sheets	Y		
2.09	MS Office Integration	Microsoft Office integration: allow input of Office documents, and must be able to work with Google Apps or Microsoft 265 solutions.	Y		
2.10	Virus Scanning	Supports virus-scanning of uploads	Y		
2.11	Historical Version Comparison	Easily compare historical versions (with and without current version) with differences highlighted. Audit trail of changes, who made them, and produce report of changes.	N		
2.12	Remote Access	Manage handheld devices remotely from an administrators desktop	Y		
2.13	Dual Synchronization	Supports both wireless and docked data synchronization	Y		
2.14	Photo Imaging	Supports the capture of digital photographs by the handheld computer/scanner	Y		
3.00	Publishing Capabilities				
3.01	Multiple Concurrent Authoring	The system must allow for multiple authoring (concurrency).	Y		
3.02	Online Forms	Ability to create online forms--no coding.	Y		
3.03	Extensible Presentation Layer	The system must have an extensible presentation layer which allows for growing the functionality of the solution through Web Service for Remote Portlets (WSRP).	N		
3.04	Workflow Processing Approval	The system must incorporate at least one level of approval workflow processing (change management).	Y		

Code	Requirement Title	Requirement Description	Must Have	Included Y/N	Vendor Response Comments
3.05	Search Engine	Incorporate a search engine capable of functioning with fuzzy logic or language-friendly terms.	N		
3.06	Automated Backup	Ability to automate archiving or automatic backup of content.	Y		
3.07	Automated Solution Log Archive	Any log that the solution creates must be automatically archived (to clear system space).	N		
3.08	Parameterized Lookups	Ability to look up data using variables from within a page/template	N		
3.09	Dynamic Online Forms/Prompts	Online forms/prompts capable of creating, receiving, and pushing data to/from multiple sources	Y		
3.10	Simultaneous Data Extract, Multiple Locations	Ability to extract data simultaneously from multiple sources for presentation on a single web page	N		
3.11	Formatting Features	List formatting features, such as spell checking, included in the solution without additional software being installed on the content-provider's desktop	Y		
3.12	Staging Environment	Solution to include a staging environment where content can be viewed in the same way as presented to the end user	Y		
3.13	Data Transfer	Two-way data push from the Infor EAM application to the hand-held device and from the handheld device to the Infor EAM application via the <i>Mobile Solution</i>	Y		
3.14	Electronic Signature	Can capture a signature electronically	Y		
3.15	Scanning	Provide advance barcode scanning support for automatic focus assignment after scanning a barcode utilizing one-dimensional or two-dimensional scanner	Y		
3.16	Lockout Capabilities	Capable of preventing users from loading unauthorized applications on the mobile devices	Y		
3.17	Software Capabilities	Supports the rapid development and deployment of applications without the use of custom code	Y		
3.18	Functionality	Capable of running on multiple devices (e.g. laptops and handhelds) without having to alter the application for each different device	Y		

Code	Requirement Title	Requirement Description	Must Have	Included Y/N	Vendor Response Comments
3.19	Data Acquisition	Gathering unlimited data fields with filtered responses through various input devices including but not limited to keyed entry, digital signature pad, magnetic strip, barcode, or photographs	Y		
3.20	Software Security	Data gathering platforms/devices must be capable of secure, wireless transmission of data to the repository and to printers; use of existing wireless infrastructure should be an option	Y		
4.00	Technical				
4.01	Certification	The system must be certified on Microsoft Windows Server, Microsoft Structured Query Language (SQL) server, and Oracle 10g and 11g platforms	Y	Test	
4.02	Administration in MS IE 7	The administration portion of the system must work in Microsoft Internet Explorer 7+.	Y	Test	
4.03	Multiple administrators/end users	The system must scale to 50 or more administrators/authors/approvers, as the solution adoption grows.	Y	Test	
4.04	Centralized Administration	Administrator must have all appropriate levels of administration.	Y	Test	
4.05	Out-of-box integration	Act as a family of products (out of the box integration, single vendor support)	Y	Demo	
4.06	Server Licensing	The solution must have a server license model (not seat).	Y	Inspect	
4.07	Multiple Languages	Support multiple languages (double-byte languages).	Y	Demo	
4.08	Version Control	Solution to include ability to lock content to ensure that simultaneous users don't overwrite each other's changes, all content provider's should be able to see their pages and only modify them if they are not checked out by another content provider	Y	Test	

ATTACHMENT C
PREVIOUS CUSTOMER REFERENCE WORKSHEET

At the time of quote submission, three references are required from Contractors that can substantiate large customer accounts where the Contractor has provided sales, service and support similar to the requirements of this bid. Please submit these references using this Attachment C, Previous Customer Reference Sheet. Only one copy of the form is provided in the RFQ package. Bidders are required to copy the form as required to meet the reference submission requirements.

[illegible]



CITY OF SAN JOSE
AIRPORT DEPARTEMENT
AIRPORT TECHNOLOGY SERVICES

**OPERATING SECURITY POLICIES:
INFORMATION SYSTEMS AND TECHNOLOGY**

October 2011



1.0 Purpose, Scope, Audience, and General Provisions	3
2.0 PCI Policy	5
3.0 Communication Rooms (MDF/IDF)	8
4.0 Airport Integrated Network (AIN) Management	11
5.0 Systems Administration	15
6.0 Data Storage, Backup and Recovery	17
7.0 Logging and Audit Trails	19
8.0 Malware Management	23
9.0 Software/Hardware Asset Control	25
10.0 Change Management	27
11.0 Information Security Incident Response	28
12.0 Airport & City User Accounts	31
13.0 End-User Equipment	33
14.0 Mobile Computers	35
15.0 Passwords	37
16.0 Internet Access	39
17.0 Remote Access for City employees	41
18.0 Network Access for non-employees	43
19.0 Handling Personally Identifiable Information (PII)	46
20.0 Definitions	50



1.0 Purpose, Scope, Audience, and General Provisions

The City of San Jose, Airport Department's intentions for publishing an Information Security Policy is to protect the City of San Jose employees, business partners and tenants from illegal or damaging actions by individuals, either knowingly or unknowingly. All of these entities utilize the Airport's infrastructure including the Premises Distribution System (cabling) and the Airport Integrated Network (AIN). Our business partners and tenants also utilize the Airport's telephony system and common use systems to conduct business at the Mineta San Jose International Airport (SJC).

These Policies as presented herein set forth security requirements to protect the use and integrity of SJC information technology equipment and systems provided and maintained by the Airport Department through its Airport Technology Services Division (ATS) or vendor support representatives hired to support IT systems on SJC's behalf.

For City of San Jose employees, these policies are in addition to any City of San Jose Policies manual, chapter 1.7 Technology policies. For any discrepancy between this policy and City of San Jose policies, the City of San Jose policy will take precedence.

Audience

The policies apply to all City employees working at SJC, consultants/contractors, and vendor support representatives. The total of all persons who utilize the SJC information technology equipment are referred in these policies as SJC Users.

Inclusion

These policies apply to all network devices, workstations, kiosks, printers, scanners, servers, applications, databases, and all other devices connected to the Airport Integrated Network (AIN). These components are defined in these policies are SJC computing systems.



Exclusions

The Public who use the Airport Free-Wifi service that is hosted by SJC on an isolated VLAN are excluded.

Airlines who utilized the SJC AIN and the AirIT shared-use environment are covered under the airline lease agreement with the airport.

These policies cover specific components of the Airport Department's Information Technology equipment and systems (presented in the following sections). Excluded is electronic mail which is already addressed by the [City of San Jose Guidelines manual, section 1.7.1](#), which all City employees and consultants/contractors with a City of San Jose email account are required to comply.

See section 19 of this document for definitions of terms used in these policies.

Policy

- 1.1 All SJC users who utilize or have access to SJC computing systems must be familiar with, and adhere to these policies.
- 1.2 SJC vendor support representatives managing IT systems on behalf of SJC must read and agree to these policies
- 1.3 These policies, including any of its component sections, will be reviewed annually and modified or updated as technology conditions change, as a result of a security assessment, or pursuant to other City of San Jose policies.
- 1.4 These policies will be posted on the SJC Intranet and provided to vendor support representatives.
- 1.5 Questions or recommendations regarding the content and implementation of these policies shall be directed to the ATS Director, Diane Mack-Williams at 408-392-1190 or dmack-williams@sjc.org.



2.0 PCI Policy

Purpose

The PCI DSS, a set of comprehensive requirements for enhancing credit card payment account data security was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for **security management, policies, procedures, network architecture, software design and other critical protective measures** to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

These standards are designed to protect cardholder information of individuals or entities that utilize a credit card to transact business with the Airport. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised from time to time by the PCI Security Standards Council.

This policy applies to sensitive data stored, processed and transmitted within or among any and all of the SJC information systems, whether individually controlled or shared, stand-alone or networked, and all computer systems and communication facilities owned, leased and operated by or on behalf of SJC. This includes, at minimum, the [Premises Distribution System](#), AIN network devices, servers, workstations, personal computers, smart phones, telephones, wireless devices and any associated peripheral equipment and software that processes credit card data.



Audience

This policy applies to all SJC users who utilize or have access to SJC computing systems & network that process, store or transmit any credit card data. Airlines & tenants that utilize the SJC AIN network should be familiar with, and adhere to applicable policies and understand the SJC commitment to PCI-DSS.

The Mineta San Jose International Airport (SJC) provides the Airport Integrated Network (AIN). This network is utilized by all entities on the SJC campus and provides Layer2 VLAN transport to all entities. SJC, as a service provider under the PCI-DSS definition must adhere to all standards of the most recent PCI-DSS requirement.

Policies

- 2.1 All credit card processing activities and related technologies must comply with the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety.
- 2.2 SJC will maintain PCI compliance as a network service provider for the Local Area Network (LAN) based on the standards of PCI-DSS.
- 2.3 Any application that processes credit cards at SJC must be certified to be PA-DSS compliant.
- 2.3 Annual PCI-DSS audits will be conducted as required by the PCI-DSS standards. At the very minimum, a self-assessment will be completed for the AIN network and any SJC applications that process credit card information.
- 2.4 Confirmation of compliance as a network service provider will be posted on the SJC website. http://www.flysanjose.com/business/tenant/N_PCI.pdf
- 2.5 Individual requirements related to PCI-DSS are addressed in other parts of the SJC Security Policy Document.
- 2.6 The SJC AIN network provides only layer2 VLANs to its partners and tenants to conduct their business. All layer3 routing will be approved by the application owner or vendor support representative.



- 2.7 The SJC Internet shall not be used to transmit credit card data. Credit card data will be transmitted over dedicated connections approved by the application owner and managed by ATS or the vendor support representative.
- 2.8 Credit card data cannot be sent via any end-user messaging technologies including email, instant messaging, etc.



3.0 Communication Rooms (MDF/IDF)

Purpose

Communication rooms (MDF/IDF) are facilities used to house the physical Airport IT systems including servers, network and other computing equipment.

Physical network security shall be used to isolate network equipment from unauthorized personnel. It is also necessary to provide a reliable environment in the communications rooms to ensure the effectiveness in the operation of the servers and network equipment.

Audience

This policy applies to any City of San Jose employee or vendor support representative needing access to any of the Airport's communication rooms.

Policy

- 3.1 Data center and telecommunication rooms are to be used for the purpose of conducting authorized business and not to be used for non-IT related activities.
- 3.2 Servers and networking equipment shall be placed in a secure room with proper access controls where physical access is limited to only authorized individuals.
- 3.3 Physical access controls must meet the most current standards of PCI-DSS.
- 3.4 An access control system device (e.g. badge reader or Cyber Lock) shall be installed at all SJC MDFs and IDFs.
- 3.5 Only authorized employees, vendor support representatives and authorized TSA employees are allowed to enter the MDF/IDF. Authorized is defined as individuals that have an airport badge and have badge access to the rooms. ATS must approve access to vendors needing access.
- 3.6 SJC vendor support representatives with badging escort privileges may provide escort to rooms housing equipment they are responsible for supporting.



- 3.7 Non-badged persons entering an MDF/IDF must have a visitor badge and must be escorted by a properly badged person. A properly badged person must have an escort sticker affixed to their badge.
- 3.8 All escorted persons entering an MDF/IDF must complete the physical paper log including name, company represented, and date, time of entrance and exit and purpose of visit. Logs will be collected quarterly and stored for 2 years.
- 3.9 Escorts must remain with the escorted person(s) at all times in an SJC communications room.
- 3.10 The access control systems shall log all access to the rooms. ATS shall review the physical access logs for the MDF/IDF quarterly or immediately after a network security incident occurs.
- 3.11 Non-badged vendor support personnel must obtain a visitor badge from the SJC front desk lobby and be escorted by a badged employee or vendor support representative at all times.
- 3.12 ATS personnel will audit SJC vendor badges quarterly that provide escorted access to the MDF/IDF rooms.
- 3.13 Equipment in MDF/IDF shall be rack mounted in the ATS assigned location. ATS shall assign rack space, ups, power source, and network jack for all equipment in the MDF/IDFs.

All equipment will be clearly labeled with system name/function and owner and contact information.
- 3.14 Trash cans are not permitted in the MDF/IDF. These must remain outside to avoid the need for janitorial staff to enter.
- 3.15 Prior to performing maintenance and or repairs to any equipment, ATS must be notified as to who will be performing the service, who the business owner is and who will be providing escorting services. This information must be tracked in the room log.
- 3.16 The MDF/IDFs shall be sufficient in cooling and electrical power to support the heat load of all the equipment. Heat sensors will be installed in all MDF/IDFs where active equipment is installed and enabled with remote



monitoring with notification to the responsible party.

- 3.17 The MDF/IDFs shall use a fire detection and suppression system. Portable fire extinguishers will be mounted in each room.
- 3.18 The network and Mission Critical & Critical SJC computing systems shall be connected to the emergency generator power.
- 3.19 The network and Mission Critical & Critical SJC computing systems shall be protected by an UPS unit.
- 3.20 UPS units shall have a minimum capacity to support the orderly system shutdown or startup procedure.
- 3.21 UPS units shall be connected to a dedicated electrical circuit.
- 3.22 UPS units shall be network monitored for events and alarms daily.
- 3.23 Airport or SJC vendor support representatives shall perform a routine preventative maintenance on the UPSs.
- 3.24 Airport or SJC vendor support representatives shall notify business system owners when servicing UPSs that impact the production environment.
- 3.25 All UPS at SJC are considered to be locked down. No devices should be plugged into an existing UPS without approval from ATS.



4.0 Airport Integrated Network (AIN) Management

Purpose

The new San Jose Airport integrated network (AIN) is designed to support shared infrastructure for all airport employees and tenants. ATS is responsible for the management and integrity of the AIN. ATS provides network services to the tenants that include network access and transport services and Voice Over IP (VOIP) telephony services.

The network is designed to provide High Availability using redundant equipment and multiple physical data paths. This policy sets forth policies relative to the management of the AIN.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of the core network and any network components attached to the network including the Wireless LAN Controller, Internet Connectivity, Firewalls, etc.

Policy

- 4.1 AIN network configuration information such as passwords, IP addresses, vlans, equipment settings, and network diagrams are classified as "Confidential" and are important to network security.
- 4.2 All network confidential documents shall have a Confidential stamp or watermark clearly displayed on the document. AIN confidential information shall not be disclosed or distributed without approval from the ATS Director.
- 4.3 Network confidential information shall not be left unattended in any non-secured work area. All network information will be stored in locked cabinets or in a locked room with access control.
- 4.4 Network confidential documents will only be stored on-line in a password protected file directory that only allows access to authorized personnel or in a fire-proof safe.



- 4.5 All production network configuration changes shall employ a formal change control procedure as outlined in policy #10 which is used to ensure that only authorized changes are made.

Network configuration changes shall be logged in the ATS change management system and kept for a minimum of one year.

- 4.6 Network configurations shall be fully documented which includes all equipment inventory, configuration, physical and logical network topology diagrams, VLAN configuration, switch configurations, etc. These documents shall be kept updated and saved as confidential information and provided to ATS. Storage location of these documents must be approved by ATS.
- 4.7 Network configurations shall be reviewed routinely by ATS.
- 4.8 Notification of network configuration changes shall be sent to all business system owners and or tenants with description of the impact to their operational environment. Notifications shall be coordinated by ATS.
- 4.9 Network equipment configuration shall follow ATS network standards.
- 4.10 Internal and external vulnerability scans will be completed on a quarterly basis or when there is a significant change in the network.
- 4.11 To ensure security and facilitate shared use of the network dedicated layer2 VLANs will be configured based on the requirements of each system or application based on the requirements of the Business Owner. Each tenant and IT system will have a separate VLAN defined to meet the needs of that system.
- 4.12 Intrusion detection and intrusion prevention software must be installed, configured and monitored on a daily basis.
- 4.13 AIN network logs must follow logging and audit requirements as identified in section 7.
- 4.14 AIN Network Engineer shall review the network logs daily and apply any necessary preventative measures. Any anomalies will be reported to the ATS Director.



- 4.15 Network configuration on firewall, IPS, switches, and routers shall be reviewed every 6 months or more frequently based on security risks identified by internal or external sources and by the Network Service Provider and ATS.
- 4.16 All network system administration processes and procedures must be compliant with the current version of PCI-DSS. In addition, testing procedure as defined in the latest PCI-DSS document must be adhered to.
- 4.17 Network activity shall be monitored 24x7 to capture performance, anomaly activities, and intrusion.
- 4.18 Firewalls will be implemented for each untrusted network such as Internet connection, City of San Jose network and between any demilitarized zone (DMZ) and the internal network.
- 4.19 File integrity monitoring software shall be used to alert personnel to any unauthorized modifications to systems that process, store or transmit any credit card data.
- 4.20 All publicly accessible network jacks must be disabled when not in use or have physical network port locks on all accessible jacks.
- 4.21 Wireless access points must be in a location that is not easily accessible. This could include ceilings, closets or hidden location.
- 4.22 ATS shall monitor Free Wi-Fi network activity 24x7 to detect rogue access points and/or intrusion. Rogue access points shall be analyzed for security events. Preventative action shall be taken to prevent network security breach.
- 4.23 No network traffic shall be allowed from the Free Wi-Fi VLAN to other AIN VLANs.
- 4.24 Access to Free Wi-Fi control system (WCS) shall only be available via direct connection.
- 4.25 For wireless environments connected to credit card data, vendor default password and settings must be changed and strong encryption



technology must be employed.

- 4.26 Airport wide scan of rogue wireless access points must be conducted on a quarterly basis.
- 4.27 Strong encryption must be used to safeguard sensitive credit card data transmitted over any wireless network.

FINAL



5.0 Systems Administration

Purpose

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of the system administration of any SJC computing system.

Policy

- 5.1 A server must not be connected to the SJC network until it is in a validated secure state and the network connection is approved by ATS.
- 5.2 All SJC computing equipment shall be configured, installed and supported according to the SJC System Administration standards and guidelines.
- 5.3 ATS or SJC vendor support representative shall routinely review the system administration and operational procedures to identify security weaknesses and implement improvement.
- 5.4 All mission critical and critical systems must follow the change management policies as defined in section 10.
- 5.5 Patch needs to be examined, and tested by ATS or SJC vendor support representative before deploying to the SJC computing systems on the AIN.
- 5.6 Any found system vulnerabilities shall be communicated immediately to the business system owner and ATS.
- 5.7 Each server must support only one primary function. (web, application,



database)

- 5.8 All computers must have the latest Service Packs and Security Patches installed. Network or system security patches shall be applied as soon as possible to prevent network security breach, at least monthly.
- 5.9 All patches beyond critical operating system and standard security patches shall be approved by change management before applying to the SJC computing system.
- 5.10 Patches shall be installed during off-business hours unless instructed by ATS or business system owner.
- 5.11 Vendor supplied passwords must be changed prior to connecting a system to the AIN.
- 5.12 All non-console administrative access shall be encrypted.



6.0 Data Storage, Backup and Recovery

Purpose

City network resources such as emails, files, databases, etc. are stored on the SJC computing systems. Protecting through appropriately backing up and archiving the files and databases is important to continuing business operations.

The purpose of this policy is as follows:

- To safeguard the information assets of San Jose Airport
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.
- To ensure PCI-DSS guidelines are followed.

This policy applies to servers and storage devices used to manage data and the backup and recovery of all systems at SJC.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of any SJC computing system.

Policy

- 6.1 All data saved on SJC owned equipment shall be for City business only.
- 6.2 ATS shall designate network resources (servers or drives) where City employees should send critical data files for inclusion in the backup process. No business files or data should be retained on a desktop C: drive or removable media (thumb drives, CDs, or DVDs) that is not being backed up.
- 6.3 All confidential City or SJC data shall be stored on SJC owned storage devices. SJC users shall not store confidential data on desktop/laptop's local or removable drives without prior authorization from Department



Director.

- 6.4 SJC users shall not save personal files on servers.
- 6.5 SJC users shall periodically review their data to meet City retention guidelines and purge all non-required documents.
- 6.6 All City employees and consultants with email access are responsible for following the City of San Jose email policy as described in the [City of San Jose Guidelines manual, section 1.7.1.](#)
- 6.7 Storing, backup and processing of any credit card data must be in compliance with the current PA-DSS and PCI-DSS standards.
- 6.8 Ensure that third parties who process customers' payment cards comply with PCI DSS, (Pin entry device) PED and/or PA-DSS as applicable.
- 6.9 Business System owner or his/her designate is responsible for ensuring an SLA is defined that provides the backup and recovery requirements for all applications/systems at SJC. This includes backing up of all files that are necessary to restore a system including data files and configuration files.
- 6.10 Backup data shall follow [City of San Jose Guidelines, Technology section 1.7.](#)
- 6.11 Any backup using tape or removable media technology shall be stored in an off-site location that is secure, protected from environmental hazards, and accessed only by authorized personnel. ATS shall approve the off-site location.
- 6.12 ATS or SJC vendor support representative shall implement a testing procedure in non-emergency situations to ensure that data, systems, and configurations are recoverable from the backup media.
- 6.13 All critical and mission critical applications will have an incident response plan. ATS or SJC vendor support representative shall routinely review the SJC system recovery plan for each critical or mission critical application to ensure staff understanding of the procedure and their responsibilities.



7.0 Logging and Audit Trails

Purpose

System Logging is a mechanism to allow IT personnel to perform system audit for access to the SJC computing systems and any system events related to hardware or software failure or intrusion, or application or user events. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. In conjunction with appropriate tools and procedures, audit trails can help information security and IT staffs detect security violations, system performance problems, and flaws in applications. Determining the cause of a compromise is very difficult without system activity logs. It is important to review system event logs and take necessary corrective procedures to prevent system failures that impact the SJC business operations.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of any SJC computing system.

Policy

- 7.1 Logging and auditing for systems that store, access or transmit credit card data must follow the most current PCI-DSS and must at least contain the following:
- Adequate logging, that covers both logged event types and details to reconstruct the following events at minimum:
 - o All individual accesses to cardholder data
 - o All actions taken by any individual with root or administrative privileges
 - o Access to all audit trails
 - o Invalid logical access attempts
 - o Use of identification and authentication mechanisms



- o Initialization of the audit logs
 - o Creation and deletion of system-level objects
 - Central log aggregation
 - Log retention (1 year with a minimum of three months immediately available for analysis)
 - Log protection and security
 - Daily log review
- 7.2 All security logs must be reviewed at least daily and that follow-up to any noted exceptions is required. Immediate communication of anomalies must be made to the ATS Infrastructure Manager.
- 7.3 Storage of audit files must be in a secured in an access-controlled room environment.
- 7.4 Logging facilities and log information should be appropriately protected against tampering and unauthorized access. This could include:
- Privacy protection measures for logged data that may be sensitive or confidential; and
 - Security protections of a technical, physical and administrative nature (e.g., division of responsibilities) to ensure integrity and availability of audit logs.
 - Control of the movement and handling of log files in order to maintain a chain of custody.
- 7.5 The time clocks for all relevant information processing systems (including systems that manage credit cards) within an organization or security domain must be appropriately synchronized with an approved time source, as part of protecting the accuracy of log information.

ATS Director shall approve the time source for any mission-critical application or application that processes credit card data.



- 7.6 When requested, and for the purpose of performing an audit, SJC users may be asked to provide information to the ATS audit team.

This access may include:

- User level and/or system level access to any SJC computing systems.
 - Access to information that may be produced, transmitted or stored on AIN network equipment or premises.
 - Access to work areas (labs, offices, cubicles, storage areas, etc.)
 - Access to interactively monitor and log traffic on AIN.
- 7.7 Network access auditing for City of San Jose employees shall be approved by the Office of Employee Relations.
- 7.8 The SJC network and SJC computing systems which support mission-critical and critical application authentication containing SJC business data, or access permission to confidential files shall have logging enabled.
- 7.9 System logs shall be reviewed by network or system administrator on daily basis.
- 7.10 Anomaly events shall be reported to the business system owner and ATS immediately.
- 7.11 Audit trail history and system logs shall be kept for a minimum of 1 year.
- 7.12 User access records shall be kept for 2 years.
- 7.13 Logging records shall have user identification, type of event, date and time of event, success or failure indication, origination of event, and identify of affected data, or system component, or resource.
- 7.14 Logging records shall be viewed by business system manager or network administrator or authorized SJC vendor support representative employee only.
- 7.15 Utilize file-integrity monitoring software and provide alerts to signal unauthorized configuration changes and modification of critical system



files. Configure the software to perform critical file comparisons at least weekly. Examples of files that should be monitored:

- System executables
- Application executables
- Configuration and parameter files
- Centrally stored, historical or archived, log and audit files



8.0 Malware Management

Purpose

Computer intruders typically use malicious software as a tool to spread computer viruses and worms. This section of the policies sets directions to minimize the installation of malicious software onto the SJC desktops/laptops. Preventing the installation of malicious software will minimize the spreading of computer viruses, worms, and other forms of malicious software ("malware", "Spyware") on the Airport Integrated Network (AIN).

This policy is designed to help prevent infection of SJC's computers and computer systems by computer viruses and other malicious code. This policy is intended to help prevent unauthorized access or damage to user applications, data, files, and hardware.

Audience

This policy pertains to all devices that connect to the AIN SJC VLANS used to conduct Airport business.

Policy

- 8.1 All computer resources attached to the SJC AIN shall be safeguarded against malicious software by having anti-malware software installed and managed as defined in this policy.
- 8.2 SJC users shall not knowingly create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of the AIN or applications.
- 8.3 SJC users shall not download any unlicensed software, MP3 music, movies, or copyrighted material onto SJC computing systems connected to the AIN.
- 8.4 Anti-malware software, and software security patches shall be installed, configured, and maintained on each SJC computing system.



- 8.5 Anti-malware software, and software security patches shall be monitored from a server console.
- 8.6 SJC users shall notify ATS immediately if the presence of malicious software is suspected on any device, and must follow all instructions provided by ATS to minimize the effect of data corruption or spreading of any malicious code.
- 8.7 The anti-virus library definitions shall be updated at least once per day.
- 8.8 Anti-virus scans must be configured to scan files in real time and full scans shall be done a minimum of once per week on all user controlled workstations and servers.
- 8.9 SJC end users shall not be able to stop anti-virus definition updates and anti-virus scans.
- 8.10 ATS or SJC vendor support representative shall monitor SJC computing systems daily to ensure systems are not infected with viruses or worms.
- 8.11 ATS or SJC vendor support representatives shall notify business system owner and perform necessary action to remove viruses and worms from the infected computing systems. If infections are found on hardware that is not directly supported by ATS, the SJC vendor support representative will notify ATS and the business owner immediately.
- 8.12 If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device will be disconnected from the network until the infection has been removed. This will be done under the direction of ATS.
- 8.13 Virus prevention training should be made available to all end users.
- 8.14 SJC users are not to perform virus recovery, removal or cleaning on their own; they should contact ATS for support. ATS will be responsible to conduct the virus identification and removal.
- 8.15 SJC users should not visit potentially hazardous web sites and should only download active content or files for business use only.



9.0 Software/Hardware Asset Control

Purpose

SJC asset control policy helps to protect the security of the AIN, protect data integrity, and protect and control computing systems and organizational assets. The asset control policy establishes how organizational assets will be tracked, who is using them and protects data being stored on those assets. This asset policy also covers disposal of assets. This section of the policies sets directions for tracking software/hardware inventory.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of any SJC computing system.

Policy

- 9.1 SJC computing hardware/software assets shall be identified, tracked and monitored.
- 9.2 All SJC computing equipment shall be identified and configured by ATS or an SJC vendor support representatives before being implemented into the production environment.
- 9.3 Each piece of equipment shall have tamper resistant tags identifying it as property of SJC.
- 9.4 Only SJC standard approved software shall be installed on any SJC equipment. All software installations shall be performed by authorized ATS or SJC vendor support representative only.
- 9.5 Software and hardware list shall be reviewed periodically to ensure accuracy.
- 9.6 Software installed on SJC computing systems shall have proof of license and an inventory of software licenses maintained by ATS or SJC vendor support representative.



- 9.7 All disposals of assets shall be inventoried and recorded before disposal.
- 9.8 Prior to disposing, recycling or donating any equipment, the hard drives must be sanitized by using a device or program designed to permanently erase the data from the drive in a secure manner.

FINAL



10.0 Change Management

Purpose

In order to ensure the stability of the AIN, a network and system configuration change control procedure is critical to the Airport.

Audience

This policy refers to the AIN network and all systems that are deemed mission critical or critical.

Policy

- 10.1 All network configuration changes that impact the AIN environment shall employ a formal change control procedure which is used to ensure that only authorized changes are made. This includes changes on network equipment, servers, applications and databases, etc.
- 10.2 All changes shall be tested successfully in a test environment before being applied to the SJC computing environment.
- 10.3 The change requester shall send notification of change to SJC users impacted before the change is implemented.
- 10.4 The change request shall include documentation of impact to the SJC computing systems, test results, and back-out procedures.
- 10.5 Any applications related to credit card processing must follow all current PCI-DSS controls for code modification, approvals and change management controls.
- 10.6 For applications that have interfaces to other systems, the enterprise change management process must be followed.



11.0 Information Security Incident Response

Purpose

IT Security Incident Response Policy is established to protect the integrity, availability and confidentiality of confidential or proprietary information to prevent loss of service and to comply with legal requirements. This policy establishes the coordination of the Airport's response to computerized and electronic communication systems incidents to enable quicker remediation.

The purpose of information security incident response is to:

- a. mitigate the effects caused by such an incident,
- b. protect the information resources of the Airport from future unauthorized access, use or damage, and
- c. ensure that SJC fulfills all of its obligations under federal and state laws and regulations with respect to such incident.

An IT Security Incident ("Incident") is any activity that harms or represents a serious threat to the whole or part of SJC's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, or a crime or natural disaster that destroys access to or control of these resources.

Audience

This policy pertains to all SJC systems and personnel involved in the management and support of the IT systems at SJC.

Policy

- 11.1 All SJC users are subject to the Acceptable Use Policy as defined within this document and employees are subject to The City of San Jose's policies as defined in the City's policy manual. The City's policy can be found in:

<http://www.csj.gov/oer/CPM/CPM171UseofEmail,InternetServices&OtherElectronicMedia.pdf>.



- 11.2 All SJC users are responsible for reporting known or suspected information security events promptly to ATS. ATS has primary responsibility for IT incident identification, remediation and serves as the primary contact for all IT security incidents.
- 11.3 ATS or SJC vendor support representatives shall follow ATS direction to perform the following activities:
- Quarantine any offending computing systems.
 - Detect or scan for virus/malware infections.
 - Update software with security patches.
 - Inspect and analyze network logs, ie firewall logs, intrusion prevention logs, server logs, etc.
 - Analyze computing system to ensure it is ready to be reconnected to the production network.
- 11.4 Specific security and incident response and escalation procedures must be developed, documented, and distributed to the appropriate personnel for all mission critical systems, the network and any applications where credit card data is processed, transmitted or stored.
- 11.5 The most recent PCI guidelines must be followed for incident response procedures.
- 11.6 System and application Business Owners are responsible to ensure that each IT system and application must have an SLA or vendor contract in place that specifies the back-up and recovery requirements, the Recovery Time Objective (RTO), Recovery Point Objective (RPO) and the level of criticality of the system. All SLAs and vendor contracts will be stored in a central location for easy reference.
- 11.7 ATS defines roles and responsibilities for ATS staff when responding to security incidents. SJC users are required to cooperate and participate in the network security incident when required.
- 11.8 Any system or network administrator who observes an intruder on the Airport network or system shall take action to terminate the intruder's access immediately. Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from



the network until the extent of the damage can be assessed. System and/or security administrators shall quickly eliminate the method of access used by the intruder and any related vulnerabilities.

- 11.9 Every effort shall be made to save log files and system files that could be used as evidence of a security incident. This includes backing up the affected environment; thoroughly documenting all activities performed on the affected platform or environment to contain, mitigate, and restore the environment. Ensure storage of any potential evidence, such as drives, diskettes, or tapes, in a locked safe; and document and control the movement and handling of potential evidence in order to maintain a chain of custody.
- 11.10 ATS shall communicate security incident information to the MOD who will in turn be responsible for all internal communications relating to the incident. The MOD will notify Business System Owners and Senior Management if mission critical systems must be taken off line to perform incident management or restoration.
- 11.11 Any public release of information concerning a computer security incident shall be coordinated by the MOD to the Airport's Public Information Officer.
- 11.12 All IT security incidents shall have a root cause analysis completed; a lesson's learned meeting and a written report detailing the findings.
- 11.13 Business System Owners shall designate one primary and one secondary system manager for all applications where they are the primary owner. Emergency contact information shall be filed with the Airport Operations Center and kept current.
- 11.14 Each mission critical and critical SJC computing system shall have a system recovery plan on file and must complete an annual test of the recovery plan. Vendor managed systems must have a system recovery plan on-file with ATS and Vendor support representatives must provide annual recovery test results to ATS.



12.0 Airport & City User Accounts

Purpose

ATS or SJC vendor support representative provides user accounts and passwords to SJC users to access the SJC network resources. A user account with a secret password is a critical security component of the AIN network. This section of the policies sets directions to minimize exposure of SJC network resources from risks associated with the misuse of SJC user accounts.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of any SJC computing systems.

Policy

- 12.1 SJC users shall be given a unique user account to access any systems connected to the AIN. The user account shall be used in conjunction with the secret password to access the AIN.
- 12.2 Only those individuals with business job requirements must have access to cardholder data. Access to credit card data by an SJC employee must be approved by the Airport Director.

Access rights for these user IDs must be set to the least privileges necessary to perform the job responsibilities.
- 12.3 Documented authorization for individuals requiring access to credit card processing applications must be completed by management and tracked and audited on a quarterly basis.
- 12.4 SJC users shall not share the user account and his/her secret password with anyone or display their assigned user account and password in the work area.
- 12.5 Inactive user accounts greater than 90 days shall be disabled and user U: files will be copied to disk and provided to the manager.



- 12.6 SJC employee's supervisor must request an employee or non-employee user account for access to the City VLANs by submitting a helpdesk request to ATS and following applicable policies. The employee must have a valid employee number issued from HR prior to the user account being set up. The manager is responsible for defining the level of access the employee is allowed.
- 12.7 Vendor support representatives must follow all PCI standards in the administration of user accounts for the systems that they are responsible for.
- 12.8 ATS or SJC vendor support representative must notify SJC user's supervisor that the user account has been created.
- 12.9 ATS or SJC vendor support representative shall immediately revoke access for any terminated SJC users.
- 12.10 Sessions that have been idle for more than 15 minutes should be timed out.
- 12.11 All documents and media containing cardholder data must be marked with a Confidential stamp or watermark clearly displayed on the document.
- 12.12 Storage of any documents or media containing cardholder data must be kept in a locked location and access to that data must be controlled. An inventory of these documents/media must be kept and examined on a quarterly basis.
- 12.13 When the documentation/media are no longer needed, the documents must be shredded and not left in a recycle location.
- 12.14 Any media containing cardholder data that is sent outside of the SJC facility must be logged and managed by a secure courier.



13.0 End-User Equipment

Purpose

SJC provides equipment to the SJC users to conduct City of San Jose and Airport business. This section of the policies sets directions for utilizing end-user equipment and requirements to protect the equipment from damage, being lost or stolen, and minimizing risks of virus infection.

Audience

Pertains to all SJC users utilizing the SJC computing environment.

Policy

- 13.1 Equipment must be connected to the AIN at the assigned network location. ATS or SJC vendor support representative is responsible for making the network connections.
- 13.2 SJC users shall not connect any personally-owned equipment to the City VLANs without ATS approval.
- 13.3 Only ATS or SJC vendor support representative is permitted to disassemble or physically modify computers, printers, network connections or other network equipment.
- 13.4 Equipment must follow Malware Management policies outlined in section 8.
- 13.5 All end-user equipment that connects to the internet must have the built-in firewall and/or a firewall application enabled .
- 13.6 Equipment assigned to security personnel, human resource administrators and system administrators, that contain confidential data, shall be configured so they cannot be booted from a floppy disk or CD ROM and passwords shall be enabled.



- 13.7 Perform a network or system lock procedure when leaving equipment unattended in the office.
- 13.8 SJC employee computers shall not have local administrative privileges to the workstations. Other computers should only have administrative privileges if absolutely required and should be coordinated with ATS.
- 13.9 Portable devices used to store SJC confidential and sensitive data must be kept physically secured by using encryption. This includes USB thumb drives, external hard drives, CDs, iPods, multimedia players, PDAs, or any device that has the capability to store data.
- 13.10 On SJC employee computers, email scanning of attachments is required and performed by the City of San Jose Information Technology Department.
- 13.11 No modems shall be installed on end-use equipment attached to the AIN unless authorized ATS.
- 13.12 Any processing of credit card data on a City of San Jose computer must be done on an isolated PC designated only for that purpose.



14.0 Mobile Computers

Purpose

This policy is designed both to protect the confidentiality of any SJC data that may be stored on a mobile computer and to protect the SJC network from being infected when the mobile computer connects to the SJC network.

Audience

This policy pertains to SJC owned laptops and end-user owned laptops and tablet computers.

Pertains to all SJC users utilizing the SJC computing environment.

Policy

- 14.1 All SJC owned mobile computers must follow Malware Management policies outlined in section 8.
- 14.2 Any SJC vendor support representatives utilizing a laptop to conduct business at SJC, must have approval by their SJC Sponsor and ATS prior to connecting to the SJC network.
- 14.3 Any laptop computer that directly connects to the City VLANS or any other VLANS on the AIN shall not have wireless adapter enabled to be connected to another network via wireless.
- 14.4 Confidential SJC business data shall not be stored un-encrypted on laptop computers.
- 14.5 All SJC owned laptops or vendor laptops that store any SJC business data shall have security software installed that will allow for remote erasing of all data should the laptop be lost or stolen.
- 14.6 SJC users wishing to connect their mobile computer to the Internet while on-site at SJC, must utilize SJC Free wi-fi service.
- 14.7 SJC users may not attach their personal laptops or tablet computers to any City vlans directly. Connection must be done according to the Remote Access policies in section 17.



- 14.8 Connection of any mobile computer to the SJC network must follow the Remote Access policies in section 17.
- 14.9 SJC issued laptops should not be left unattended. They must be locked in secure areas, or transported with the end user. Loaner laptops will be stored in a locked room.

FINAL



15.0 Passwords

Purpose

Passwords are an important aspect of network security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the SJC computing assets. All SJC users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This section of the policies sets directions to minimize exposure of AIN or SJC network resources from risks associated with the misuse of passwords.

Audience

This policy applies to any City of San Jose employee or vendor support representative responsible for the management of any SJC computing system.

For City of San Jose employees, this policy is in addition to any City of San Jose Policies manual, 1.7.1 Use of Email, Internet Services & Other Electronic Media

Policy

- 15.1 SJC users shall implement a complex password to access the AIN. A complex password is a pass-phrase with a minimum of 8 characters having at least a combination of three of the following four categories:

Alpha letters in uppercase and lowercase, numbers, and non-alphanumeric special character format.
- 15.2 SJC users shall change network access password every 6 months. Old passwords shall not be reused in 24 password change intervals. Any user account that is used to process credit cards must be changed every 90 days.
- 15.3 SJC users shall not share the password with anyone or display their assigned password in the work area. It is recommended that the password not be written down anywhere in the work area.



- 15.4 SJC users must change their passwords immediately if they believe that their password may have been disclosed/compromised by unauthorized individuals.

If they believe that their password has been compromised, please notify ATS.

- 15.5 SJC users must request a password reset by notifying ATS or SJC vendor support representative. SJC users shall not request a password reset on behalf of another SJC user.

ATS or SJC vendor support representative will reset the password and communicate it to the employee's voice mail account only.

- 15.6 ATS or SJC vendor support representative must validate the request for a password reset. The validation may be accomplished by a telephone call via a work phone to the employee or employee's supervisor. ATS or SJC vendor support representative shall not create or reset employee passwords without appropriate validation.

- 15.7 ATS may conduct a password cracking exercise as part of a security audit. When such an activity occurs, ATS shall send a notification to SJC users and SJC business owners in advance. SJC users may be required to change passwords immediately after completion of a security audit.

- 15.8 Vendor-supplied default passwords shall be changed using a complex password before installing a system on the AIN.

- 15.9 User accounts shall be disabled after five repeated attempts with the wrong password.



16.0 Internet Access

Purpose

SJC provides Internet connectivity for the SJC City vlan users to conduct the City and the Airport business. This section of the policies sets directions for accessing information from the Internet and preventing inappropriate Internet usage.

Audience

This policy pertains to any SJC user needing access to the Internet.

For City of San Jose employees, this policy is in addition to any City of San Jose Policies manual, 1.7.1 Use of Email, Internet Services & Other Electronic Media

If there are any discrepancy between this policy and City of San Jose policies, the City of San Jose policy will take precedence.

Policy

- 16.1 SJC equipment or systems that have access to the Internet shall have installed anti-virus software with the latest security pattern files, security patches, and firewall protection.
- 16.2 SJC users are responsible for all Internet activities and its content that occurs on their assigned SJC computing systems.
- 16.3 Internet access is set up by default on all SJC employee computers. Requests for terminating Internet connectivity privileges shall be submitted by the employee's supervisor to ATS by a service desk ticket. The request shall include identification of the specific user, computer and location.
- 16.4 ATS shall implement Internet filtering to prevent access to unauthorized websites per City of San Jose Internet policy. The Internet filtering definition shall be updated as determined necessary by ITD, ATS or Airport management.
- 16.5 SJC may terminate or refuse to extend Internet access to any SJC



computing system that is compromising the AIN or SJC network resources.

- 16.6 SJC may terminate or refuse to extend Internet access to any SJC user who using a SJC computing system to provide Internet connectivity to an unauthorized party including family members, or connecting an unauthorized computer to the AIN network without approval from SJC, or conducting personal business with inappropriate websites.
- 16.7 City employees shall have no expectation of privacy in their usage of the Internet. Internet emails, attached files, or other materials transmitted over the Internet can be monitored, or stolen by intruders.
- 16.8 SJC computing systems that have access to the Internet shall be made available immediately to ATS or SJC vendor support representative for inspection when requested.
- 16.9 When surfing on the Internet, only visit sites that you are familiar with and do not click on any on-line programs, attempt to install any files or click to accept an offer of any sort. Malicious code can be downloaded to your PC without your knowing.
- 16.10 No credit card data may be transmitted over the SJC Internet. All credit card transmissions must be encrypted and sent over isolated data connections (e.g. dsl line).



17.0 Remote Access for City employees

Purpose

Remote access connectivity to City VLANs may be necessary for City employees to perform Airport business functions. This remote access policy is designed to provide necessary access while preventing any security risks or damage to the AIN or SJC computing systems and to prevent compromise or loss of data.

This section of the policies defines guidelines for network connectivity and security standards for a computer connecting to the AIN from outside of the airport.

This policy assumes that the user's computer equipment is owned personally by them and is installed at their home or used outside of the Airport premises.

Audience

This policy pertains to any City of San Jose employee needing access to the City VLANS at SJC.

This policy is in addition to the City of San Jose Policies manual, 1.7.3 Remote Access. If there are any discrepancies between this policy and City of San Jose policies, the City of San Jose policy will take precedence.

Policy

- 17.1 In order to be eligible for a remote access VPN connection, SJC user shall have an AIN network account; submit a remote access VPN request form approved by division Deputy Director, Business System Owner, (if applicable) and ATS or SJC vendor support representative.
- 17.2 SJC users are responsible for all activities and content that occurs within their computers while connecting to the AIN via remote access VPN. It is the responsibility of the SJC user to understand his/her computing system configuration and settings in order to troubleshoot any remote access VPN connectivity issue from remote locations.



- 17.3 Remote access equipment shall have anti-virus software running in real time with the latest definition files, and updated software security patches, and protection by an ISP firewall, a properly configured hardware or software firewall.
- 17.4 VPN connections using a public computer or device such as kiosk computers at Internet cafes, conferences, or training centers, are not permitted.
- 17.5 ATS or SJC vendor support representative may terminate or refuse to extend a remote access VPN connection to any SJC user if the connection compromises the AIN.
- 17.6 Remote access connection shall be automatically disconnected after 30 minutes of inactivity.
- 17.7 A semi-annual audit will be conducted for all users who have been given permission to have remote access to the City VLANS.
- 17.8 Two-factor authentication is required for all remote access for any employees having access to credit card data.
- 17.9 All remote access connection requests must be documented per the remote access procedure and shall be approved by ATS or SJC vendor support representative via the change management procedure before any remote access connection be made.
- 17.10 Transmission of passwords must be encrypted using strong cryptography.



18.0 Network Access for non-employees Consultants/Contractors/vendors

Purpose

The Airport Department's consultants, contractors and vendors need access to the City network resources such as applications, emails, files and project information to conduct official City and Airport business. In addition, vendor support representatives require access to the AIN to provide support for systems they have been contracted to support.

Audience

This section pertains to consultants/contractors/vendors with current City contracts and who are required to access the Airport's network resources in order to perform services for the Airport.

Policy

- 18.1 City consultants/contractors/vendors that require access to the AIN shall have an SJC sponsor. The sponsor must be the Deputy Director of an Airport division or Assistant Director. The sponsor shall be responsible for consultant/contractor/vendor computer activities while connected to the Airport's network.
- 18.2 For access to the City VLANs, SJC sponsor must complete the non-employee new user request in the ATS service desk intranet page. The request will generate a non-disclosure agreement that must be printed and signed by the non-employee, their supervisor, and the deputy director of the Airport division that is sponsoring them. The service desk request must list what access privileges are required.
- 18.3 The sponsor will be responsible for informing ATS when non-employees no longer work at the airport through the separation form on the ATS Service Desk. This notice must be completed within 24 hours of departure to protect network resources.
- 18.4 City consultants/contractors/vendors shall not connect company or personal equipment directly to the Airport's network, nor shall they use



any SJC computing system to access his/her own company network while at Airport facilities.

- 18.5 City consultants/contractors/vendors shall not remove any assigned SJC computing systems from Airport facilities.
- 18.6 Airport sponsor/divisions shall not implement any network connectivity setup for consultants/contractors/vendors without prior written approval from ATS.
- 18.7 City consultants/contractors/vendors must have approval from the sponsor and the ATS Division Manager prior to setting up his/her own technology equipment at City facilities. Sponsor may request internet access to connect to their corporate computer systems or use SJC free wi-fi.
- 18.8 It is the responsibility of consultants/contractors/vendors to understand his/her personal computing system configuration and settings in order to troubleshoot any computer issues. ATS has the discretion to not provide technical support to any non-ATS hardware equipment or software.
- 18.9 City consultants/contractors/vendor shall abide by all applicable City of San Jose policies and Airport policies including any non-disclosure agreements that may be applicable.
- 18.10 For access to City VLANs, ATS will manage all non-employee network accounts in separate Organizational Unit (OU) in Active Directory. Each individual company will be set up in a separate OU.

Vendor remote access lists will be reviewed quarterly by ATS, and a listing of active accounts will be sent to the sponsor for review and continued approval.
- 18.11 Non-employees who require access to any City documents should have these documents available to them through a SharePoint Intranet Team Site set up by the sponsoring division.
- 18.12 Access to business applications will be granted by the Business Owner for that application.



- 18.13 Sponsor will submit a completed Request for VPN connectivity form and a service desk ticket to ATS requesting remote access VPN connectivity for the vendor support representative.
- 18.14 SJC Network Engineer shall document and keep all VPN configurations for security auditing in a secure location designated by ATS management.
- 18.14 VPN documentation shall be confidential and shall only be accessible by authorized employees.
- 18.15 For contractors/consultants/vendors that have remote access, the business owner is required to submit a service desk request to terminate access when contractor/consultant is no longer working at the airport.
- 18.16 Accounts used by vendors for remote access must only be enabled during the time period needed. Monitor vendor remote access accounts when in use.
- 18.17 All SJC equipment including spares to support operational needs will be housed physically at SJC and will be kept in a location approved by SJC.



19.0 Handling Personally Identifiable Information (PII)

Purpose

The escalation of security breaches involving personally identifiable information (PII) has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Organizational harms may include a loss of public trust, legal liability, or remediation costs.

There are numerous Federal and California laws relative to the handling of Personally Identifiable Information including:

- [Privacy Act of 1974](#), as amended
- [Federal Information Security Management Act \(FISMA\)](#) (January 2003)
- California
 - o The California state constitution declares privacy an inalienable right in Article 1, Section 1.
 - o [California Online Privacy Protection Act \(OPPA\) of 2003](#)
 - o [SB 1386](#) requires organizations to notify individuals when PII is known or believed to be acquired by an unauthorized person.
 - o In 2011, the California State Supreme Court ruled that a person's ZIP code is PII.

There are also Proposed Federal Bills that could further impact PII:

- [Privacy Act of 2005](#)
- [Information Protection and Security Act](#)
- [Identity Theft Prevention Act of 2005](#)
- [Online Privacy Protection Act of 2005](#)
- [Consumer Privacy Protection Act of 2005](#)
- [Anti-phishing Act of 2005](#)
- [Social Security Number Protection Act of 2005](#)
- [Wireless 411 Privacy Act](#)



Consequences

There are also financial implications for not complying with PII laws. Per the Privacy act;

Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of the Privacy Act shall be guilty of a misdemeanor and fined not more than \$5,000.

Audience

This section pertains to any SJC user who is involved in processing any PII data and all systems that store or process PII information.

Additional information is available at:

http://www.rsa.com/solutions/pii/sb/10206_PII_SLG_SB_0409.pdf

Policy

19.1

SJC must follow industry accepted PII principles as defined in NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122). <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

19.2

SJC must minimize the use, collection, and retention of PII to what is strictly necessary to accomplish the business purpose and mission. On a semi-annual basis:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete
- Reduce PII holdings to the minimum necessary for proper performance of SJC functions
- Establish a plan to eliminate the unnecessary collection and use of SSNs.

19.3

PII data shall be stored on network drives and/or in application databases



with proper access controls (i.e., User IDs/password) and shall be made available only to those individuals with a valid need to know.

PII data may not be stored on any user workstations or mobile devices including, but not limited to, notebooks computers, USB drives, CD-ROMs/DVDs, etc. without the direct permission of the Director.

Any PII data approved by the Director to be stored outside of the application database must be encrypted using a FIPS 140-2 certified encryption module.

No employee or contractor shall physically take PII information from SJC facilities or access remotely without permission from the Director.

- 19.4 Any employee handling PII information should be required to be trained on the proper management, storage, retention and destruction of the data.
- 19.5 Any incident involving data breaches which could result in identity theft must be communicated to the Director's office and ATS immediately. An incident response team must identify the nature of the breach and proper notification of the breach must follow state and federal regulated notification.
- 19.6 Hard copy reports that contain PII data must be stored in a locked cabinet and follow any City related retention policies. At no time should any PII data be left unattended.
- 19.7 If PII needs to be transmitted over the Internet, it must be sent encrypted.
- 19.8 An incident plan to handle breaches involving PII should be completed and tested.
- 19.9 Securely delete PII when there is no longer a business need for its retention on computing systems. (This includes extra copies, backups and data that has exceeded its required retention period.)

For paper copies, always shred or otherwise destroy PII before disposing



of it.

For computers or printers that have a hard drive, the drive must be securely wiped prior to disposal.

FINAL



20.0 Definitions

AIN	SJC Airport Integrated Network. This is a shared network supporting airport business, airline shared use, airline back office computing and other tenant computing. The AIN is managed as a PCI compliant network and utilizes layer2 VLAN technology to isolate independent businesses data.
Anti-virus/Anti-malware/Anti-spyware	Special software to protect the information and data stored in the SJC business systems including desktops, laptops and servers from unwanted malicious software.
ATS	Airport Technology Services. This is the SJC IT organization responsible for setting standards, monitoring compliance and managing day-to-day production environment for City of San Jose business systems.
Business System Owner	SJC Deputy Director who has the prime responsibility for the use of the computer system to meet the operational needs of their division. They are responsible for overseeing the operational state of the owned system or application.
Business System Manager	SJC user who has responsibility of functionally administering and managing SJC computing system. This is typically a direct report of the SJC Deputy Director.
Critical	Those systems or system components that they business deems as critical to the organization's success and area heavily relied upon in day-to-day business. If these systems are inoperable or inaccurate for greater than 6-8 hours, they would cause great disruption to the organization. There are some manual work processes to compensate if the system or system component is



unavailable, and loss of up to 6-8 hours of data could be recreated.

Desktop	Computer assigned to the employees to work at the Airport Department facilities and also refers to any PC used in support of business operational systems including the shared-use systems at gates, ticket counters and FIDS system.
Firewall	A hardware device or software to filter network traffic from and to the SJC computing devices configured only to allow approved network traffic and protocols from specific locations. .
Intruders	Unauthorized access individuals who attempted to make configuration changes or access the information or data stored in the SJC desktops, laptops, servers or other network devices.
IP	Internet Protocol – A computer protocol that specifies the way data is broken into packets for transmission.
Mission-critical	Those systems or system components that the business deems as vital to the organization and that if they are inoperable or inaccurate for any length of time would cause great disruption to the organization. There are minimal or no manual work processes that could be put in place. A mission-critical system or system component requires immediate recovery to the minute with no data loss.
Network	A collection of computers and devices interconnected by communications channels that facilitate communications and allows sharing of resources and information.
Non-Critical	Systems or system components that assist the day-to-day business by automating routine functions. They may only be used under certain circumstances or times of the year. If they are inoperable or inaccurate for greater than 5 days would cause some disruption to the organization.



There are manual work processes or data downloads to spreadsheets or secondary data sources that could assist in the recovery of the data. Data loss of up to 48 hours could be recreated or tolerated.

Password/Passphrase	Special words, phrase, or sentence required to be entered to access the SJC AIN network and systems.
PII - Personally Identifiable Information	The term Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
Remote Access VPN	A method to remotely and securely access the SJC network via the Internet.
Security Patches	Special software required to be installed periodically onto the SJC desktops, laptops, or servers or other computing devices to fix identified security vulnerabilities
Server	A computer, or series of computers, that link other computers or electronic devices together. They often provide essential services across a network, either to private users inside an organization or to public users via the internet. Many servers have dedicated functionality such as web servers, print servers, and database servers.
SJC Users	City of San Jose employees, Airport consultants, contractors, system support provider, who have access to the AIN network. This also pertains to airline personnel who utilize the SJC AIN network for shared-use. (do we include airlines in this definition?)



SJC vendor support representative	A vendor who provides support services for SJC computer systems or network. The SJC vendor support representatives have obligations to administer, and manage SJC computing system per SJC policies, standards and guidelines. A support contract defines their level of responsibility, SLA, etc.
UPS – Uninterruptible Power Supply	An electrical apparatus that provides emergency power to electronic and computer equipment when the input power source fails. A UPS differs from an auxiliary or emergency power system or standby generator in that it will provide instantaneous or near-instantaneous protection from input power interruptions by means of one or more attached batteries and associated electronic circuitry.
User Account	Special identification used by a person to authenticate to the SJC computing systems and be granted authorization to access specific data or functions of the systems.
Telecommunication rooms (MDF/IDF)	Secured rooms within the Airport property that house the Airport network, equipment and cabling.
Viruses/Worms	Unwanted malicious software used to obtain unauthorized access, vandalize, corrupt or damage the computer systems. Intruders can use this software to take control of the computers remotely.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network



Acknowledgement & Agreement

Name _____

Company _____

Division/Section (SJC Employees Only) _____

Badge Number _____

Supervisor or Airport Sr. Staff Sponsor _____

I, _____ certify that I have read the Airport Information Security Policies and that I will abide by these policies as part of my required daily work.

Name Printed: _____

Signature: _____

Date: _____

Supervisor or Sponsor:

Name Printed: _____

Signature: _____

Date: _____

Question and Answers for Bid #RFQ 15414 - Mobile Solutions Application

OVERALL BID QUESTIONS

Question 1

Attachment A:

1. Para 4.6, appears they are requesting both thick and thin (browser and mobile device view ability)? We did not originally quote the Thin Client. Is this what is meant by this requirement?
2. Para 10.1 requests 7:00 AM to 7:00 PM toll free phone support. Is 8:00 to 6:00 acceptable?

Attachment B:

1. Para 1.08, Must include analytics tool capable of tracking users¿ navigation throughout the application. Do not understand what this means. We currently have date and time stamps for every ¿touch¿ on the device in the field, does this suffice?
2. Para 1.11, Meet the City¿s security standard relative to information security, ¿ what is the standard?
3. Para 2.07, The resulting web sites must function equally well in either graphical or text-only mode. What does this mean? What web site?
4. Para 2.09, MS Office integration, allow input of Office documents, and must be able to work with Google Apps of MS 265 solutions....we allow file attachments, does this suffice?
5. Para 2.10, Support virus scanning uploads? MobileFrame is a self-contained system. We can coexist with Virus scanning software, does this suffice?
6. Para 3.05, Incorporate a search engine capable of functioning with fuzzy logic or language friendly terms. What is intended by this requirement? We can call third party apps from within MobileFrame, does this suffice? **(Submitted: Apr 2, 2012 2:29:58 PM PDT)**

Answer

- 1. Para 4.6, Currently the airport utilizes Internet Explore 7.0 for its Internet connection and all field devices will be required to have the capabilities to utilize the Internet from the field for researching equipment/manufacture specifications.
 - 2. Para 10.1, Since the airport is a 24/7 daily operation we require as much toll free telephone support as needed. The hours of 8:00AM to 6:00PM daily will suffice, and would require an escalation plan during non-supported telephone times.
- Attachment B:
1. Para 1.08, The application should have the capabilities of tracking user devices for transactional auditing, accountability, and troubleshooting electronic records¿.
 2. Para 1.11, The link for this document is located on the airport Intranet site and cannot be accessed through the Internet. See Airport Security PDF file.
 3. Para 2.07, The Mobile Solution needs to function through any airport website is required for the application to function properly.
 4. Para 2.09, Documents must be of a type that is compatible with the application to consist of but not limited to Adobe PDF, MS Office, *.TIF, and *.JPEG for pictures.
 5. Para 2.10, ? Any application that resides on a city or airport support server/computer must be able to function fully and properly without any degradation while the application is being monitored and/or scanned by the network virus scanning software, along with any and all transmission of data.
 6. Para 3.05, Should an end user require searching for information pertaining to a work request/order, then application must have the capabilities to do the search as if they were at an actual computer utilizing simple word terms or identifiers. **(Answered: Apr 3, 2012 2:48:17 PM PDT)**

Question 2

Will the City agree to use the current contracts the vendor has in place if awarded the business? **(Submitted: Apr 4, 2012 11:06:44 AM PDT)**

Answer

- All software agreements between the City and Vendors must be reviewed and approved by the City¿s Attorney, and the terms and conditions of the City¿s purchase orders attached to this quote shall apply. **(Answered: Apr 5, 2012 10:25:21 AM PDT)**

Question Deadline: Apr 9, 2012 1:00:00 PM PDT