# Solicitation RFP-PRO-FY13-0009

# Mobile Device Management System

## County of Santa Clara

# Bid RFP-PRO-FY13-0009
# Mobile Device Management System

| | |
|---|---|
| Bid Number | **RFP-PRO-FY13-0009** |
| Bid Title | **Mobile Device Management System** |
| Bid Start Date | **Jul 27, 2012 9:10:43 AM PDT** |
| Bid End Date | **Aug 22, 2012 3:00:00 PM PDT** |
| Question & Answer End Date | **Aug 2, 2012 3:00:00 PM PDT** |
| Bid Contact | **Caroline Kho**<br>**Procurement Contract Specialist**<br>**408-491-7428**<br>**Caroline.Kho@proc.sccgov.org** |

**Description**

The County of Santa Clara (hereafter, “County") is requesting proposals from qualified suppliers to provide a mobile device management platform, which may include design, implementation and training services.

Facing a growing demand and the increased complexity of mobile computing, the County seeks a tool to securely manage County owned as well as County employees' personal mobile device environment consisting of 4,400 smart and feature phone (cellular only) devices. It is projected that most feature phones will be replaced by smartphones. Current mobile security practices are marginal and lacking in enterprise grade management and security functionality thereby inhibiting increased mobile adoption.

A mobile device management (MDM) platform will be the first strategic enabler within the County's overall mobile strategy. The expectation is that the MDM platform will help manage the transition to a heterogeneous mobile computing and communications environment allowing the use of popular smartphone and tablet operating systems (OS) over a secure and managed foundation.

MDM implementation is targeted for Fall of 2012.

The proposed system should help the County realize the following organizational benefits:

a. Increased flexibility when selecting smartphone OS's

b. Additional mobile functionality

c. Increased productivity and satisfaction due to a flexible mobile environment

d. Implementation of industry standard enterprise grade mobile security to mitigate risks to County networks and data

e. Facilitates the adoption of a Bring-your-Own-Device (BYOD) strategy to further increase efficiency and user satisfaction and decrease costs

f. Existence of a real-time, centralized tool to administer mobile devices throughout the enterprise with comprehensive monitoring and reporting capability

g. Capability to adapt to future changes in mobility as market conditions evolve

The County will consider a county-hosted solution or an Application Service Provider (ASP) vendor hosted solution. Offerors may submit only one proposal. The proposal may include one type of solution or both types of solutions.

The proposed solution(s) must have the capability to:

- Manage Apple iOS phone and tablet operating systems; AND
- Manage Google Android phone and tablet operating systems; AND
- Support Microsoft Office 365

Proposals not meeting this mandatory requirement will be excluded from further evaluation.

The proposed solution shall be a proven system with a track record of large successful deployments. The County is not interested in beta systems or purchasing professional services to design and develop a system. The integrated solution must meet the technical, support, service, and business requirements as defined in this RFP.

This RFP may result in a single source award.

The resulting contract shall be for a term of three (3) years with an option to renew for two (2) additional years, unless terminated earlier or otherwise amended.

# COUNTY OF SANTA CLARA, CALIFORNIA

## REQUEST FOR PROPOSAL NO. RFP-PRO-FY13-0009

## FOR
## MOBILE DEVICE MANAGEMENT SYSTEM

**ISSUED:**
July 27, 2012

**PROPOSALS DUE DATE:**
August 22, 2012 by 3:00pm PACIFIC TIME

**PROCUREMENT DEPARTMENT**
**2310 NORTH FIRST ST., SUITE 201**
**SAN JOSE, CA 95131-1040**

Caroline Kho
Procurement Contracts Specialist
(408) 491-7428 or caroline.kho@proc.sccgov.org

# TABLE OF CONTENTS

# TABLE OF CONTENTS

*continued*

## ATTACHMENTS

*The attachments listed below are for reference only and do not have to be submitted with the proposal.*

# I. INTRODUCTION

## A. INVITATION

The County of Santa Clara (hereafter, “County”) is requesting proposals from qualified suppliers to provide a mobile device management platform, which may include design, implementation and training services.

Facing a growing demand and the increased complexity of mobile computing, the County seeks a tool to securely manage County owned as well as County employees’ personal mobile device environment consisting of 4,400 smart and feature phone (cellular only) devices. It is projected that most feature phones will be replaced by smartphones. Current mobile security practices are marginal and lacking in enterprise grade management and security functionality thereby inhibiting increased mobile adoption.

A mobile device management (MDM) platform will be the first strategic enabler within the County’s overall mobile strategy. The expectation is that the MDM platform will help manage the transition to a heterogeneous mobile computing and communications environment allowing the use of popular smartphone and tablet operating systems (OS) over a secure and managed foundation.

MDM implementation is targeted for Fall of 2012.

The proposed system should help the County realize the following organizational benefits:

a. Increased flexibility when selecting smartphone OS’s
b. Additional mobile functionality
c. Increased productivity and satisfaction due to a flexible mobile environment
d. Implementation of industry standard enterprise grade mobile security to mitigate risks to County networks and data
e. Facilitates the adoption of a Bring-your-Own-Device (BYOD) strategy to further increase efficiency and user satisfaction and decrease costs
f. Existence of a real-time, centralized tool to administer mobile devices throughout the enterprise with comprehensive monitoring and reporting capability
g. Capability to adapt to future changes in mobility as market conditions evolve

<u>The County will consider a county-hosted solution or an Application Service Provider (ASP) vendor hosted solution. Offerors may submit only one proposal. The proposal may include one type of solution or both types of solutions.</u>

<u>The proposed solution(s) must have the capability to:</u>

- Manage Apple iOS phone and tablet operating systems; AND
- Manage Google Android phone and tablet operating systems; AND
- Support Microsoft Office 365

Proposals not meeting this mandatory requirement will be excluded from further evaluation.

INTRODUCTION

The proposed solution shall be a proven system with a track record of large successful deployments. The County is not interested in beta systems or purchasing professional services to design and develop a system. The integrated solution must meet the technical, support, service, and business requirements as defined in this RFP.

This RFP may result in a single source award.

The resulting contract shall be for a term of three (3) years with an option to renew for two (2) additional years, unless terminated earlier or otherwise amended.

## B. BACKGROUND

### 1. County of Santa Clara

Santa Clara County (SCC) is the fifth most populous County in California, with a population of nearly 1.8 million people. The County contains fifteen cities, encompassing approximately 1,300 square miles, which have large concentrations of electronics, research and manufacturing firms. Santa Clara County is the fifth-largest County government in the State and has an estimated workforce of 15,000.

The County organizational structure includes a decentralized mix of approximately fifty (50) semi-autonomous County Agencies and Departments. The County provides services such as public safety and justice, road construction and maintenance, parks and recreation, libraries, and environmental resource management. It also operates "enterprise" programs, which charge fees to users for services. Two examples are the Santa Clara Valley Medical Center and the County airports. The County acts as an agent of the State in administering health, social services, and criminal justice programs that are of statewide concern.

The County is governed by a five member Board of Supervisors who is elected by district to serve four-year terms. The County Executive administers the day-to-day affairs of the County and is appointed by the Board of Supervisors.

### 2. County Information Technology (IT) Environment

The Office of the Chief Information Officer (CIO) coordinates County information technology planning and management and promotes the collaboration of County Agencies and Departments in the development of enterprise-wide information systems. The CIO manages the Information Services Department (ISD) which performs information and technology systems planning, development, acquisition, implementation, and maintenance for a majority of County Departments. Some Agencies, such as the Santa Clara Valley Health and Hospital System (SCVHHS) and the Social Services Agency (SSA) maintain their own information technology staff and systems, but collaborate with ISD in Countywide technology projects.

## 3. Technical Environment

### SANTA CLARA COUNTY INFORMATION SERVICES DEPARTMENT

**Technical Standards – Intel Platform**

### SERVER

| | |
|---|---|
| Operating system | Windows Server 2003/2008/2008R2 |
| LDAP Servers | Microsoft Active Directory Services<br>Sun Directory Server |
| Hardware | Intel-Based Servers with multiple processors (redundant), SAN integration via Emulex 1000-L2 HBAs, redundant power supplies.<br>Virtual Appliance (OVF) |
| Hypervisors | VMware ESX 4/4i |
| Backup | IBM TSM Client 5.4.x, CA ARCServe |
| Application Servers | .NET Framework 4.0/3.5/3.5SP1<br>Java Runtime Environment 1.5/1.6 |
| Databases | Microsoft SQL Server 2005/2008/2008 R2 (32 & 64 bit)<br>Oracle v8, 9, 10, & 11 |
| High Availability and Clustering | HA Clustering and FT Supported |
| Disk array | Raid 1(Blade),Standalone: RAID 1 (OS) RAID 5 (Data) |
| Antivirus | Symantec AV 12.x |

### PC HARDWARE/SOFTWARE

| | |
|---|---|
| Desktops | HP Business Line Desktops |
| Laptops | HP and Lenovo Line Notebooks |
| Monitors | 17”-30” Monitors |
| Docking station | Basic and Advanced docking stations |

### MOBILE DEVICE HARDWARE/SOFTWARE

| | |
|---|---|
| Hardware | Apple iPhone and iPad, Google Android based phones and tablets, Microsoft Windows Phone 6.x |
| Operating System | IOS 4.x, 5.x, Android ICS+ and Honeycomb+, Windows Phone 6+ |
| Email | Microsoft Outlook 2003/2010 |

### PRINTERS

| | |
|---|---|
| Laser | HP LaserJet devices<br>Ricoh MFP devices |
| Network interface | HP- Internal Jet Direct<br>Ricoh internal network interface |

### COMMUNICATION

| | |
|---|---|
| Protocol | TCP/IP |
| Topology | Ethernet |
| Routers/ switches | Cisco |
| Bandwidth – network | Gigabit (sx/lx) |
| Bandwidth – to the desktop | 10/100/1000 MB/ second |
| Backbone | Fiber optic |
| Cable to the desktop | Category 5e UTP with RJ45 connections |

### REMOTE ACCESS & AUTHENTICATION

| | |
|---|---|
| Cisco ASA VPN<br>Juniper SSL VPN<br>Citrix Netdirect<br>RSA Security Tokens<br>SecurAuth Two-Factor Authentication | Microsoft UAG for ActiveSync<br>Blackberry Enterprise Server<br>Authentication is integrated with Microsoft Active Directory (County has multiple AD forests but is working towards consolidation). |

## C. PROJECT SCOPE OF WORK

This solicitation is for a mobile device management platform which is to include all software and support services required to install and operate the proposed system on-premise or as a software as a service solution. On-premise solutions will use County supplied hardware. The complete scope of work is dependent upon the chosen solution. The installation may consist of planning, organizing and implementing the base system on Contractor supplied equipment and integrating this with County supplied equipment; training County technical support staff in the use and operation of the system; and providing technical support and maintenance upgrades. Interfaces or data file uploads from several existing systems may also be required.

## D. POINT OF CONTACT:

The County has designated a Procurement Officer who is responsible for the conduct of this procurement whose name, address and telephone number is listed below:

Caroline Kho, Procurement Contracts Specialist
County of Santa Clara Procurement Department
2310 North First Street, Suite 201
San Jose, CA 95131-1040
Telephone: 408-491-7428
Fax: 408-938-2804
E-mail: caroline.kho@proc.sccgov.org

Any inquiries or requests regarding this procurement must be submitted to the Procurement Officer in writing. Offerors may contact ONLY the Procurement Officer regarding this RFP.

# II. CONDITIONS GOVERNING THE PROCUREMENT

This section of the RFP contains the anticipated schedule for the procurement and describes the procurement events as well as the conditions governing the procurement.

## A. SEQUENCE OF EVENTS AND CONTACT INFORMATION

The Procurement Officer will make every effort to adhere to the following *anticipated* schedule:

| | **Action** | **Date** |
|---|---|---|
| 1. | Issue of RFP | **July 27, 2012** |
| 2. | Deadline To Submit Written Questions | August 2, 2012 at 3:00pm Pacific Time |
| 3. | Response to Written Questions/RFP Addendum | August 9, 2012 |
| 4. | Deadline for Submission of Proposals | **August 22, 2012 at 3:00pm Pacific Time** |
| 5. | Proposal Evaluation | August 23, 2012 thru September 10, 2012 |
| 6. | Selection of Shortlist, if applicable | September 11, 2012 |
| 7. | Demonstrations/Presentations (County option), if applicable | September 17, 2012 |
| 8. | Selection of Finalist for Negotiations, if applicable | September 28, 2012 |
| 9. | Final Negotiations or BAFO, Finalize and Award Contract | October 19, 2012 |
| 10. | Commencement of Contract | November 1, 2012 |
| 11. | Anticipated Go-Live Date | November 15, 2012 |

## B. EXPLANATION OF EVENTS

### 1. ISSUE OF RFP

This RFP is being issued by the County of Santa Clara Procurement Department. Copies of this RFP including supporting documents may be obtained from Bidsync's web site at http://www.bidsync.com

### 2. DEADLINE TO SUBMIT WRITTEN QUESTIONS

FOR QUESTIONS DUE on the deadline to submit written questions as specified in Paragraph A, Sequence of Events and Contact Information, CONTACT Caroline Kho at caroline.kho@proc.sccgov.org or (408) 491-7428.

Potential Offerors may submit written questions to this RFP until the deadline as indicated in Section II, Paragraph A. The Procurement Officer will not respond to questions **submitted in any other manner or format.**

Answers to questions received by the deadline will be listed on an addendum to the RFP and posted on the bid management site http://www.bidsync.com. Additional written questions must be received by the Procurement Officer no later than two (2) days after the addendum is posted. The County will respond in the same manner. Thereafter, the

County does not guarantee that it will respond to questions submitted before the RFP closing date and time.

## 3. RESPONSE TO WRITTEN QUESTIONS/RFP AMENDMENTS

Written responses to written questions regarding the substance of the RFP, and any material changes to the RFP, will be issued as an addendum, and posted on http://www.bidsync.com. The County reserves the right to post addenda until the RFP closing date and time.

## 4. SUBMISSION OF PROPOSAL

Proposals must be received **no later than the deadline specified in paragraph A of Section II.** All received proposals will be time stamped.

All deliveries via express carrier should be addressed as follows:

Caroline Kho, Procurement Contracts Specialist – **RFP-PRO-FY13-0009**
Procurement Department
County of Santa Clara
2310 North First St., Suite 201
San Jose, CA 95131-1040

Proposals must be sealed and labeled on the outside of the package to clearly indicate that they are in response to the RFP # and title as referenced on the cover page.

## 5. PROPOSAL EVALUATION

An Evaluation Committee will review and evaluate the proposals and make a recommendation for an award.

## 6. SELECTION OF SHORT LIST *{If applicable}*

Offerors that demonstrate their capacity, ability and capability to meet the County's requirements will be determined to be within the competitive range and selected on the shortlist of Offerors to progress to the next round of evaluation.

## 7. DEMONSTRATIONS/PRESENTATIONS *{If applicable}*

At County's option, Offerors may be required to perform a demonstration/presentation of their proposed solution. Demonstrations/presentations will be held on-site at a County location. The date, time, and location are to be determined.

## 8. SELECTION OF FINALIST FOR NEGOTIATIONS *{If applicable}*

At County's option, one or more Offerors may be selected as finalists and invited to enter into negotiations with the County and/or proceed to the next round of evaluations.

### 9. FINAL NEGOTIATIONS or BAFO, FINALIZE AND AWARD CONTRACT

At County's option, one or more Offerors may be selected to enter into final negotiations with the intent of award. At the County's option, Offerors may be given an opportunity to provide a Best and Final Offer.

### 10. COMMENCEMENT OF CONTRACT

The date the contract will become effective.

### 11. ANTICIPATED GO-LIVE DATE

The date the new system is expected to be operational and in production mode.

## C. GENERAL

### 1. INCURRING COST

This RFP does not commit the County to award, nor does it commit the County to pay any cost incurred in the submission of the Proposal, or in making necessary studies or designs for the preparation thereof, nor procure or contract for services or supplies. Further, no reimbursable cost may be incurred in anticipation of a contract award.

### 2. CLAIMS AGAINST THE COUNTY OF SANTA CLARA

Neither your organization nor any of your representatives shall have any claims whatsoever against the County or any of its respective officials, agents, or employees arising out of or relating to this RFP or these RFP procedures, except as set forth in the terms of a definitive agreement between the County and your organization.

### 3. GUARANTEE OF PROPOSAL

Responses to this RFP, including proposal prices, will be considered firm and irrevocable for one-hundred and eighty (180) days after the due date for receipt of proposals and/or one-hundred eighty (180) days after receipt of a best and final offer, if one is submitted.

### 4. BASIS FOR PROPOSAL

Only information supplied by the County in writing by the Procurement Officer in connection with this RFP should be used as the basis for the preparation of Offeror's proposal.

### 5. FORM OF PROPOSALS

No oral, telephone, facsimile, or electronic proposals will be accepted.

## 6. AMENDED PROPOSAL

An Offeror may submit an amended proposal before the deadline for receipt of proposals. Such amended proposals must be complete replacements for a previously submitted proposal and must be clearly identified in a written format. The County personnel will not merge, collate, or assemble proposal materials.

## 7. WITHDRAWAL OF PROPOSAL

Offerors will be allowed to withdraw their proposals at any time prior to the deadline for receipt of proposals. The Offeror must submit a written withdrawal request signed by the Offeror's duly authorized representative addressed to the Director of Procurement and submitted to the Procurement Officer.

## 8. LATE RESPONSES

In order for a proposal to be considered, the proposal must be received in person or via courier or mail to the place specified above no later than the RFP due date and time. The Procurement Department time and date stamp will be the basis for determining timeliness of proposals.

## 9. NO PUBLIC PROPOSAL OPENING

There will be no public opening for this RFP.

## 10. CALIFORNIA PUBLIC RECORDS ACT (CPRA)

All proposals become the property of the County, which is a public agency subject to the disclosure requirements of the California Public Records Act ("CPRA"). If Contractor proprietary information is contained in documents submitted to County, and Contractor claims that such information falls within one or more CPRA exemptions, Contractor must clearly mark such information "CONFIDENTIAL AND PROPRIETARY," and identify the specific lines containing the information. In the event of a request for such information, the County will make best efforts to provide notice to Contractor prior to such disclosure. If Contractor contends that any documents are exempt from the CPRA and wishes to prevent disclosure, it is required to obtain a protective order, injunctive relief or other appropriate remedy from a court of law in Santa Clara County before the County's deadline for responding to the CPRA request. If Contractor fails to obtain such remedy within County's deadline for responding to the CPRA request, County may disclose the requested information.

Contractor further agrees that it shall defend, indemnify and hold County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and attorneys fees) that may result from denial by County of a CPRA request for information arising from any representation, or any action (or inaction), by the Contractor.

## 11. CONFIDENTIALITY

All data and information obtained from the County of Santa Clara by the Offeror and its agents in this RFP process, including reports, recommendations, specifications and data, shall be treated by the Offeror and its agents as confidential. The Offeror and its agents shall not disclose or communicate this information to a third party or use it in advertising, publicity, propaganda, or in another job or jobs, unless written consent is obtained from the County. Generally, each proposal and all documentation, including financial information, submitted by an Offeror to the County is confidential until a contract is awarded, when such documents become public record under state and local law, unless exempted under CPRA.

## 12. ELECTRONIC MAIL ADDRESS

Most of the communication regarding this procurement will be conducted by electronic mail (e-mail). Potential Offerors agree to provide the Procurement Officer with a valid e-mail address to receive this correspondence.

## 13. USE OF ELECTRONIC VERSIONS OF THE RFP

This RFP is being made available by electronic means. If accepted by such means, the Offeror acknowledges and accepts full responsibility to insure that no changes are made to the RFP. In the event of conflict between a version of the RFP in the Offeror’s possession and the version maintained by the Procurement Department the version maintained by the Procurement Department must govern.

## 14. COUNTY RIGHTS

The County reserves the right to do any of the following at any time:

a. Reject any or all proposal(s), without indicating any reason for such rejection;
b. Waive or correct any minor or inadvertent defect, irregularity or technical error in a proposal or the RFP process, or as part of any subsequent contract negotiation;
c. Request that Offerors supplement or modify all or certain aspects of their proposals or other documents or materials submitted;
d. Terminate the RFP, and at its option, issue a new RFP;
e. Procure any equipment or services specified in this RFP by other means;
f. Modify the selection process, the specifications or requirements for materials or services, or the contents or format of the proposals;
g. Extend a deadline specified in this RFP, including deadlines for accepting proposals;
h. Negotiate with any or none of the Offerors;
i. Modify in the final agreement any terms and/or conditions described in this RFP;
j. Terminate failed negotiations with an Offeror without liability, and negotiate with other Offerors;
k. Disqualify any Offeror on the basis of a real or apparent conflict of interest, or evidence of collusion that is disclosed by the proposal or other data available to the County;
l. Eliminate, reject or disqualify a proposal of any Offeror who is not a responsible Offeror or fails to submit a responsive offer as determined solely by the County; and/or
m. Accept all or a portion of an Offeror’s proposal.

## 15. ASSIGNMENT OF CLAYTON ACT, CARTWRIGHT ACT CLAIMS

In submitting a response to a solicitation issued by the County, the responding person and/or entity offers and agrees that if the response is accepted, it will assign to the County all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the responding person and/or entity for sale to the County pursuant to the solicitation document. Such assignment shall be made and become effective at the time the County tenders final payment to the responding person and/or entity.

# III. RESPONSE FORMAT AND ORGANIZATION

This section contains relevant information Offerors should use for the preparation of their proposals.

## A. NUMBER OF RESPONSES

Offerors must submit only one proposal. However, an Offeror may propose a County hosted solution, an Application Service Provider (ASP) solution or both solutions. If multiple options are proposed, the Offeror must clearly identify their intent and respond using the applicable documents and forms.

## B. ORIGINAL AND COPIES

Offerors must provide one (1) original and six (6) identical copies of their proposal to the location specified on or before the closing date and time for receipt of proposals.

The original binder/submittal must be stamped "ORIGINAL" and contain original signatures on the necessary forms. The remaining sets should be copies of the originals.

Offerors must also provide two (2) electronic copies of their proposal in CD-ROM format, readable by Microsoft Office 2003 (Word, Excel and Project) software. **The two (2) CDs shall be included in the ORIGINAL binder.**

## C. PROPOSAL FORMAT

All proposals shall be typewritten on standard 8 ½ x 11 paper (larger paper is permissible for charts, spreadsheets, etc.) and placed within a binder with tabs delineating each section. Hard copies should utilize both sides of the paper where practical.

### 1. LETTER OF TRANSMITTAL

Each proposal received must include a letter of transmittal. The letter of transmittal should:

a. Identify the submitting organization;
b. Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized by the organization to contractually obligate the organization;
c. Identify the name, title, telephone and fax numbers, and e-mail address of the person authorized to negotiate the contract on behalf of the organization;
d. Identify the names, titles, telephone and fax numbers, and e-mail addresses of persons to be contacted for clarification;
e. Be signed by the person authorized to contractually obligate the organization; and
f. Acknowledge receipt of any and all addenda to this RFP; and identify all sections of the proposal that the Offeror claims contain "proprietary" or "confidential" information.

## 2. PROPOSAL ORGANIZATION

The proposal should be organized and indexed in the following format and must contain, at a minimum all listed items in the sequence indicated:

Tab 1: Letter of Transmittal
Tab 2: Table of Contents
Tab 3: Executive Summary
Tab 4: Section V – A: Offeror's Corporate Information, ***Items 1 – 6***
Tab 5: Appendix A1 and/or Appendix A2: Technical Requirements Response Form
Tab 6: Appendix B1 and/or Appendix B2: Functionality and Integration Response Form
Tab 7: Appendix C1 and/or Appendix C2: Implementation, Project Management, Training and On-going Support Response Form
Tab 8: Appendix E: Non-collusion Declaration Form
Appendix F: Declaration of Local Business, if applicable.
Tab 9: Appendix G: ASP Checklist Assessment Checklist, if applicable.
Tab 10: Appendix H: Offeror's Terms and Conditions

**APPENDIX D (D1 and/or D2) – PROPOSAL COST RESPONSE FORM**

*Offeror must submit its proposed system and services solution and price structure. The ORIGINAL document must be submitted in a sealed envelope marked "APPENDIX D - ORIGINAL." In addition, Offeror must submit two (2) copies in a separate sealed envelope marked "APPENDIX D - COPIES."*

## 3. PROPOSAL PREPARATION INSTRUCTIONS

Within each section of their proposal, Offerors should address the items in the order in which they appear in this RFP. All forms provided in the RFP shall be thoroughly completed and included in the appropriate section of the proposal.

## 4. NON-CONFORMING SUBMISSIONS

A submission may be construed as a non-confirming proposal, ineligible for consideration or incomplete if it does not comply with the requirement of this RFP.

# IV. EVALUATION

## A. FACTORS

The **Evaluation Criteria** listed below will be utilized in the evaluation of the Offeror's written proposals and demonstration/presentation accordingly. The expectation is that those proposals in the competitive range may be considered for contract award. The proposal should give clear, concise information in sufficient detail to allow an evaluation based on the criteria below. An Offeror must be acceptable in all criteria for a contract to be awarded to that Offeror whose proposal provides the best value to the County.

1. Corporate strength, experience, financial strength, references and reputation of Offeror;
2. Ability to meet technical requirements;
3. Ability to meet functionality and integration requirements;
4. Methodology for implementation, project management, training, and ongoing support; and
5. Local Preference.

*The overall total cost to the County will be considered and the degree of the importance of cost will increase with the degree of equality of the proposals in relation to the other factors on which selection is to be based*.

## B. LOCAL BUSINESS PREFERENCE

In accordance with applicable sections of Board Policy, Section 5.3.13, in the formal solicitation of goods or services, the County of Santa Clara shall give responsive and responsible Local Businesses the preference described below.

"Local Business" means a lawful business with a physical address and meaningful "production capability" located within the boundary of the County of Santa Clara.

The term "production capability" means sales, marketing, manufacturing, servicing, or research and development capability that substantially and directly enhances the firm's or bidder's ability to perform the proposed contract. Post Office box numbers and/or residential addresses may not be used as the sole bases for establishing status as a "Local Business."

In the procurement of goods or services in which best value is the determining basis for award of the contract, five percent (5%) of the total points awardable will be added to the Local Business score.

When a contract for goods or services, as defined in this policy, is presented to the Board of Supervisors for approval, the accompanying transmittal letter shall include a statement as to whether the proposed vendor is a Local Business, and whether the application of the local preference policy was a decisive factor in the award of the proposed contract.

This Local Business preference shall not apply to the following:

1. Public works contracts,
2. Where such a preference is precluded by local, state or federal law or regulation,
3. Contracts funded in whole or in part by a donation or gift to the County where the special conditions attached to the donation or gift prohibits or conflicts with this preference policy.

The donation or gift must be approved or accepted by the Board of Supervisors in accordance with County policy, or

4. Contracts exempt from solicitation requirements under an emergency condition in accordance with board policy, state law and/or the County of Santa Clara Ordinance Code (Section A34-82).

In order to be considered for Local Preference, proposer must complete and submit Declaration of Local Business with its RFP response.

# V. REQUIREMENTS AND OFFEROR SUBMITTAL

This section contains requirements and relevant information Offerors should use for the preparation of their proposals. Offerors should thoroughly respond to each requirement.

## A. OFFEROR'S CORPORATE INFORMATION

### 1. EXECUTIVE SUMMARY

Include an executive summary which should be a one or two page summary intended to provide the Evaluation Committee with an overview of the significant business features of the proposal.

### 2. OFFEROR EXPERIENCE/INFORMATION

The Offeror shall include in their proposal a statement of relevant experience. The Offeror should thoroughly describe, in the form of a narrative, its experience and success as well as the experience and success of subcontractors, if applicable in providing and/or supporting the proposed system.

In addition, Offerors are required to provide the following information:

a. Offerors shall provide the company name, business address, including headquarters, all local offices, co-location locations (city/state), and telephone numbers.

b. Offerors shall provide the length of time they have been providing their solution including any ASP and/or vendor hosted services, if applicable.

c. Offerors shall indicate any offices or facilities located within the County of Santa Clara that substantially and directly enhances the Offeror's ability to perform the proposed contract.

d. Offerors shall provide a description of the Offeror's organization, including names of principals, number of employees, client base, areas of specialization and expertise, and any other information that will assist the Evaluation Committee in formulating an opinion about the stability and strength of the organization.

e. Offerors shall provide the name of the jurisdiction in which the Offeror is organized and the date of such organization.

f. Offerors shall provide a description of the depth of their experience with providing installation services / assistance and supporting the proposed system.

g. Offerors shall provide a discussion of the type and duration of the business relationship with the manufacturer(s) whose products are included in the proposed systems.

h. Offeror must identify the physical location of the application and data storage facilities if an ASP or cloud based solution are proposed.

i. Offeror shall describe the method used for change management and advance notification timeframe for application changes.

j. Offeror shall describe the data security guarantee (data encryption, data mining, and data mismanagement penalties (leakage, etc.) if an ASP or cloud based solution is proposed.

k. Provide a complete disclosure if Offeror, its subsidiaries, parent, other corporate affiliates, or subcontractors have defaulted in its performance on a contract during the past five years which has led the other party to terminate the contract. If so, identify the parties involved and the circumstances of the default or termination.

l. A list of any lawsuits filed against the Offeror, its subsidiaries, parent, other corporate affiliates, or subcontractors in the past five years and the outcome of those lawsuits. Identify the parties involved and circumstances. Also, describe any civil or criminal litigation or investigation pending.

m. Offeror shall list and describe their top three comparative advantages over its competitors.

n. Offeror shall list and describe applicable patents.

o. Offeror shall disclose any publicly pending acquisitions.

## 3. FINANCIAL STABILITY/OFFEROR FINANCIAL INFORMATION

Offeror shall submit copies of the most recent years independently audited financial statements, as well as those for the preceding three years, if they exist. The submission shall include the audit opinion, balance sheet, income statement, retained earnings, cash flows, and notes to the financial statements. If independently audited financial statements do not exist for the Offeror, the Offeror shall state the reason and, instead, submit sufficient information such as the latest Dun and Bradstreet report to enable the Evaluation Committee to determine the financial stability of the Offeror. The Procurement Officer may request and the Offeror shall supply any additional financial information requested in a timely manner.

## 4. PAST PERFORMANCE (REFERENCES)

The Offeror’s proposal shall include three different external references from clients who have completed their projects in the last three years, who are willing to validate the Offeror’s past performance on similar projects of size and scope. The minimum information that shall be provided for each client reference follows:

1. Name of the contact person;
2. Name of the company or governmental entity;
3. Address of the contact person;
4. Telephone number of contact person;
5. Email address of the contact person;
6. A description of the services provided and dates the services were provided;

### 5. INDEMNITY AND INSURANCE REQUIREMENTS

Offerors shall provide a certificate(s) of insurance or a copy insurance declaration page(s) with their proposals as written evidence of their ability to meet the insurance certificate and other applicable County insurance requirements in accordance with the provisions listed in Attachment 2 of the RFP. In addition, Offerors should provide a letter from an insurance agent or other appropriate insuring authority documenting their willingness and ability to endorse their insurance policies making the County an additional insured.

### 6. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT AND HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

If an ASP / cloud based solution is proposed, explain if the proposed solution meets the Health Insurance Portability and Accountability Act (HIPAA) requirements and Health Information Technology for Economic and Clinical Health Act Business Associate Requirements (Attachment 3).

## B. TECHNICAL REQUIREMENTS (*APPENDIX A*)

The County is seeking a contractor to provide a complete solution to satisfy the technical, functionality, and integration requirements and one who is capable of providing the stated capacity and service levels as well as the training and technical support required to maintain the system in an operational status.

The technical requirements are to be defined referencing the requirements in Appendices A1 and A2. Offerors submitting a proposal for an on premise solution (i.e., a system located on County network) must submit Appendix A1; whereas Offerors submitting a proposal for an ASP solution must submit Appendix A2. Offerors submitting a proposal for both types of solutions must submit both appendices.

Offerors must submit a thorough narrative supported by references to the technical documentation in response to questions asked in Appendix A1 and/or Appendix A2.

## C. FUNCTIONALITY AND INTEGRATION REQUIREMENTS (*APPENDIX B*)

The County is seeking a contractor to provide a complete solution to satisfy the technical, functionality, and integration requirements and one who is capable of providing the stated capacity and service levels as well as the training and technical support required to maintain the system in an operational status.

The functional and integration requirements are to be defined referencing the requirements in Appendices B1 and B2. Offerors must complete and submit with their proposals the functional and integration requirements referenced in Appendix B1 and B2. Offerors submitting a proposal for a county-hosted solution must submit Appendix B1; whereas Offerors submitting a proposal for an ASP solution must submit Appendix B2. Offerors submitting a proposal for both types of solutions must submit Appendix B1 and Appendix B2.

## D. **<u>IMPLEMENTATION, PROJECT MANAGEMENT, TRAINING, AND ONGOING SUPPORT (*APPENDIX C*)</u>**

The implementation, project management, training, and ongoing support requirements are to be defined referencing the requirements in Appendices C1 and C2. Offerors submitting a proposal for a client server solution must submit Appendix C1; whereas Offerors submitting a proposal for an ASP solution must submit Appendix C2. Offerors submitting a proposal for both types of solutions must submit Appendix C1 and Appendix C2.

Offerors must submit a thorough narrative supported by references to the implementation, project management, training, and ongoing support in response to questions asked in Appendix C1 and/or Appendix C2.

## E. **COST PROPOSAL (*APPENDIX D1 or D2*)**

Offerors shall complete all pages of the respective Proposal Cost Response Form and submit it in a sealed envelope with their proposal. The proposed costs shall directly relate to the Project Work Plan.

## F. **OTHER SUBMITTALS**

### 1. **NON-COLLUSION DECLARATION *(APPENDIX E)***

Offerors shall complete and submit Non-collusion Declaration form with their proposal.

### 2. **DECLARATION OF LOCAL BUSINESS (*APPENDIX F)***

Offerors shall complete and submit Declaration of Local Business form with their proposal, if applicable.

### 3. **ASP SECURITY ASSESSMENT CHECKLIST (*APPENDIX G)***

Offerors shall complete and submit the ASP Security Assessment Checklist form with proposal, if applicable.

## 4. OFFEROR'S TERMS AND CONDITIONS (*APPENDIX H*)

Should Offerors object to any of the County's terms and conditions listed in Attachment A, Offerors must propose specific alternative language and indicate the reason for their objection. The County may or may not accept the alternative language. General references to the Offeror's terms and conditions or attempts at complete substitutions are not acceptable to the County. Offerors must provide a brief discussion of the purpose and impact, if any, of each proposed changed followed by the specific proposed alternate wording.

In addition, Offerors must submit with their proposal any additional terms and conditions that they expect to have included in the contract negotiated with the County. Offerors must provide specific proposed wording and a brief discussion of the purpose and impact, if any. Include any applicable agreement, such as license, service level, maintenance, etc.

# APPENDIX A1
# TECHNICAL REQUIREMENTS RESPONSE FORM FOR A COUNTY HOSTED SOLUTION

If proposing a county hosted (client/server) solution, please complete and submit Appendix A1 with your proposal.

## A. TECHNICAL REQUIREMENTS

### 1. Description of System

a. Provide a description of the proposed product, database, software and services, including how the proposed system will meet or exceed the requirements stated in the entire RFP. Include sufficient technical information about the application, operating environment and performance data to enable the County to determine whether or not the proposed system meets the technical environment prerequisites.

b. Identify/list all software required for the solution that is not supplied directly by the Offeror (any/all third party software).

c. Provide a case study for a successful MDM system implementation used by a government agency of comparable size.

d. Provide an overview and/or benchmarks relating to the system's ability to process information in real time. Include the number of concurrent users as well as named users the proposed system will accommodate and state the maximum number of recommended users.

e. Identify any requirement to purchase interfaces from other vendors to work with the proposed solution.

f. Define the scalability of the proposed system.

i. Can the system be purchased in modules and expanded?
ii. How scalable is the proposed software regarding the number of users?
iii. Does the system scale in parallel, i.e. can additional application servers be configured in a load-balanced cluster?
iv. Can the database, application and data analysis components be configured to reside on separate independent servers, so that one impacted subsystem does not affect the overall solution?

g. Describe licenses required for the software (concurrent / per seat and the number associated).

h. Define the requirements for a test system. Include all related components (hardware, software, etc.) Include test system costs.

i. Define which third party reporting tools the system is compatible with the proposed system.

j. Describe the process for change management or customer notification.

k. Describe the current generally available (GA) version number and release date, including how often new GA releases with new services and features are made available.

l. Describe how continuous application and system support is provided 24 hours a day, 365 days per year. Describe the process for requesting support during standard business hours and after hours.

m. Provide the company escalation and response plan, and describe how issues are triaged and escalated.

n. Describe the level of customization available without a programmer or vendor support.

o. Provide the location of the closest service representative.

p. Define the system uptime. Include planned downtime windows.

## 2. <u>Equipment and Software</u>

a. Provide detailed server hardware specifications, including but not limited to:
   i. operating system,
   ii. processors type and speed,
   iii. redundancy
   iv. system configuration
   v. hard drive size

b. Include a list of all hardware and software components the County must purchase.

c. Describe the proposed system architecture.

d. Describe how the client software and agent components are able to coexist with other software and applications on end-user devices.

e. Describe any maintenance and support the client is expected to do.

## 3. <u>Backup/Recovery</u>

a. Describe the backup capabilities for the proposed system.

b. Describe the process for automatic reprogramming and/or recovery after a failure due to hardware, software or absence of power.

c. Describe the capabilities for periodically exporting data stored in the database, and if it can be exported to MS Excel, MS Access or other software.

## 4. Network/Hardware

a. Discuss how the proposed solution will be able to operate within the County's Technical Environment as listed in Section I.B.3, Introduction/Background/Technical Environment, of the RFP.

b. Provide a system/network design diagram, which provides a visual summary of the system's servers, network and ancillary components and their relationships.

c. Describe any proprietary equipment utilized.

d. Describe any special networking requirements, i.e. dedicated/segregated network segments, VLANs, etc.

## 5. Storage

a. Explain how data is archived (e.g., on demand, automatically, via optical disk, etc.)

b. Describe how the system will store the data on non-proprietary media and in an industry-standard format. Offeror should also specify the type of media used for long-term storage and the format in which it is stored.

c. Describe the archival scheme for the system, including the recommended length of time data is retained on the production system and the availability of data for reporting after archiving.

d. Describe the maximum size of the database and the largest currently operating production and archive directories.

e. Describe the long-term storage options available for the system.

f. Describe how the system will print information on demand. Offeror must specify any special hardware or required printers necessary for printing.

g. Explain how long batches (batch processing data) remain in the system.

## 6. Integration

a. Describe if the system supports a web-based front end or if a client install is required.

b. Define the system's capability to support multiple browser types (i.e. Internet Explorer, Mozilla Firefox, and Opera) on different platforms, and the minimum version of each browser supported if the system supports web-based access.

c. Specify all browser plug-ins necessary to utilize web-based features.

## 7. Critical Updates, Patches and Antivirus

a. Describe the process for approving and installing operating system Critical Updates. Attach the Offeror policy regarding Microsoft Critical Updates.

b. Describe or attach the company Service Pack policy for the proposed solution.

c. Describe the Antivirus software used to protect data in real-time on the vendor's servers.

d. Describe any issues that may occur when running Antivirus software in real-time on devices.

e. Describe or attach the company policy regarding the use of anti-virus software with the proposed system.

f. Describe the disclosure policies related to security vulnerabilities found in the system, including procedures in place to notify customers of potential flaws, and the average time between a flaw being discovered and corrective action taken.

## 8. Application Security Features

a. Describe the system's compliance with LDAP (Lightweight Directory Access Protocol), and how the system can be configured to authenticate users against it.

b. Describe how the proposed solution can be configured to authenticate users against an Active Directory tree, if possible.

c. Describe how the solution audits user access and privilege use and the information that is logged.

d. Describe how the solution allows the County to configure minimum password difficulty requirements, and password lockout policies.

e. Describe how the solution allows system administrators to set a password expiration policy, thereby requiring end-users to change their passwords at a specified interval.

f. Describe how the solution encrypts sensitive information transmitted across the network and internet, and specify the algorithms used.

g. Specify whether the system establishes user identity via:

   i. A user ID and password; or
   ii. Two-factor authentication, such as a smart-card and a PIN. If two-factor authentication is available or used, Offeror must describe the hardware requirements, the authentication process, and any supplies needed for ongoing implementation.

h. Describe how access privileges are configured in the system, and whether or not privileges can be based on group designations.

i. Describe how different levels of security and privileges are established.

j. Specify if a "user inactivity timeout" feature is available that forces a user to re-authenticate if idle for a preconfigured amount of time.

k. Describe how the system utilizes electronic signatures and electronic confirmation (if applicable).

## 9. Escrow

a. Explain your company's ability to make available a software escrow account and include the source code and all products released during the maintenance term, including third party software. List the products that your company will hold in an escrow account and a list of those products that cannot be held and explain why.

b. Explain in detail the process to retrieve the software source code.

c. Provide written evidence of ability to provide and maintain a Software Escrow account in the form of a letter from an escrow agent or other acceptable third party.

# APPENDIX A2
# TECHNICAL REQUIREMENTS RESPONSE FORM FOR AN ASP (VENDOR HOSTED) SOLUTION

If proposing an ASP solution, please complete and submit Appendix A2 with your proposal.

## A. TECHNICAL REQUIREMENTS

### 1. Description of System

a. Provide a description of the proposed product, database, software and services, including how the proposed system will meet or exceed the requirements stated in the entire RFP. Include sufficient technical information about the application, operating environment and performance data to enable the County to determine whether or not the proposed system meets the technical environment prerequisites.

b. Identify/list all software required for the solution that is not supplied directly by the Offeror (any/all third party software).

c. Provide a case study for a successful MDM system implementation used by a government agency of comparable size.

d. Provide an overview and/or benchmarks relating to the system's ability to process information in real time. Include the number of concurrent users as well as named users the proposed system will accommodate and state the maximum number of recommended users.

e. Identify any requirement to purchase interfaces from other vendors to work with the proposed solution.

f. Define the scalability of the proposed system.

   i. Can the system be purchased in modules and expanded?
   ii. How scalable is the proposed software regarding the number of users?
   iii. Does the system scale in parallel, i.e. can additional application servers be configured in a load-balanced cluster?
   iv. Can the database, application and data analysis components be configured to reside on separate independent servers, so that one impacted subsystem does not affect the overall solution?

g. Identify how many users are can access the proposed system. (Concurrent users).

h. Describe licenses required for the software (concurrent / per seat and the number associated).

i. Define the requirements for a test system. Include all related components (hardware, software, etc.) Include test system costs.

j. Define which third party reporting tools are compatible with the proposed system.

k. Describe the process for change management or customer notification.

q. Describe the current generally available (GA) version number and release date, including how often new GA releases with new services and features are made available.

l. Describe how different versions of the application are managed across customer environments in the ASP, and how version migrations are managed.

m. Describe how continuous application and system support is provided 24 hours a day, 365 days per year. Describe the process for requesting support during standard business hours and after hours.

n. Provide the company escalation and response plan, and describe how issues are triaged and escalated.

o. Provide the average response time of the proposed system.

p. Describe the level of customization available without a programmer or vendor support.

q. Provide the location of the closest service representative.

r. Define the system uptime. Include planned downtime windows.

2. **<u>Equipment and Software</u>**

a. Provide detailed workstation hardware specifications, including but not limited to, operating system, RAM, size of the hard drive, type of monitors, barcode devices, scanning devices, barcode printing devices, etc.

b. Provide detailed hardware specifications for any customer-hosted components being proposed.

c. Describe how the <u>client</u> software components are able to coexist with other software and applications on end-user devices.

d. Describe the proposed system architecture.

e. Describe hardware support and escalation process for any customer-hosted components.

f. Describe any customer required maintenance/support tasks, and any relevant maintenance schedules.

## 3. Backup/Recovery

a. Describe the backup capabilities for the proposed system, including:

i. Process for how backups are performed
ii. Process for Tenant-initiated backups
iii. Service availability guarantee

b. Describe in detail your company's Disaster Recovery plan, including requirements for zero-downtime.

c. Describe the notification provided if an application failure occurs.

d. Describe the process for automatic reprogramming and/or recovery after a failure due to hardware, software or absence of power.

e. Describe the capabilities for periodically exporting data stored in the database, and if it can be exported to MS Excel, MS Access or other software. Specify supported export formats (i.e. Excel, CVS, etc.)

## 4. Network/Hardware

a. Discuss how the proposed solution will be able to operate within the County's Technical Environment as listed in Section I.B.3, Introduction/Background/Technical Environment, of the RFP.

b. Provide a system/network design diagram, which provides a visual summary of the system's servers, network and ancillary components and their relationships.

c. Describe any proprietary equipment utilized.

d. Describe any special networking requirements, i.e. dedicated/segregated network segments. VLANs, etc.

## 5. Storage

a. Explain how data is archived (e.g., on demand, automatically, via optical disk, etc.)

b. Describe how the system will store the data on non-proprietary media and in an industry-standard format. Offeror should also specify the type of media used for long-term storage and the format in which it is stored.

c. Describe the archival scheme for the system, including the recommended length of time data is retained on the production system and the availability of data for reporting after archival.

d. Describe the maximum size of the database and the largest currently operating production and archive systems.

e. Describe the long-term storage options available for the system.

f. Describe how the system will print information on demand. Offeror must specify any special hardware or required printers necessary for printing

g. Explain how the data is stored within the database, including if it can be stored in a separate database for disparate customers and/or locations. Explain how data from multiple tenants/customers is segregated and arranged.

h. Explain how the information can be retrieved from the archive.

i. Explain how long batches remain in the system.

j. Explain how, upon request or in the event of contract termination, all County data and documents stored in the system will be delivered or made available to the County in a format suitable for import into another system.

### 6. Data Management

a. Describe the data management approach.

b. Explain if the data is stored in separate databases.

c. Provide a copy of the Service Level Agreement.

### 7. Integration

a. Define the system's capability to support multiple browser types (i.e. Internet Explorer, Mozilla Firefox, and Opera) on different platforms, and the minimum version of each browser supported if the system supports web-based access.

b. Specify all browser plug-ins necessary to utilize web-based features.

### 8. Critical Updates, Patches and Antivirus

a. Describe the process for approving and installing operating system Critical Updates. Attach the Offeror policy regarding Microsoft Critical Updates.

b. Describe or attach the company Service Pack policy for the proposed solution.

c. Describe the Antivirus software used to protect data in real-time on the vendor's servers.

d. Describe any issues that may occur when running Antivirus software in real-time on devices.

e. Describe or attach the company policy regarding the use of anti-virus software with the proposed system.

f. Describe the disclosure policies related to security vulnerabilities found in the system, including procedures in place to notify customers of potential flaws, and the average time between a flaw being discovered and corrective action taken.

## 9. Application Security Features

a. Describe the system's compliance with LDAP (Lightweight Directory Access Protocol), and how the system can be configured to authenticate users against it.

b. Describe how the proposed solution can be configured to authenticate users against an Active Directory tree, if possible.

c. Describe how the solution audits user access and privilege use and the information that is logged.

d. Describe how the solution allows the County to configure minimum password difficulty requirements, and password lockout policies.

e. Describe how the solution allows system administrators to set a password expiration policy, thereby requiring end-users to change their passwords at a specified interval.

f. Describe how the solution encrypts sensitive information transmitted across the network and internet, and specify the algorithms used.

g. Describe how access privileges are configured in the system, and whether or not privileges can be based on group designations.

h. Describe how different levels of security and privileges are established.

i. Specify if a "user inactivity timeout" feature is available that forces a user to re-authenticate if idle for a preconfigured amount of time.

j. Describe how the system utilizes electronic signatures and electronic confirmation (if applicable).

## 10. Security

a. Describe network security features used to protect customer data/information (i.e. firewalls, network segmentation, etc.)

b. Explain the type of physical security used to protect customer information in vendor data centers and co-location facilities.

c. Explain the type of electronic security used (i.e. biometrics, authentication and surveillance) at vendor and co-location facilities.

d. Explain how the security and confidentiality of the system data collected and entered into the system will be maintained.

e. Describe, in detail, how County data will be partitioned from other customer's information. Include information on whether separate database containers are used.

f. Complete and submit the ASP Security Assessment Checklist.

## 11. Escrow

a. Explain your company's ability to make available a software escrow account and include the source code and all products released during the maintenance term, including third party software. List the products that your company will hold in an escrow account and a list of those products that cannot be held and explain why.

b. Explain in detail the process to retrieve the software source code.

c. Provide written evidence of ability to provide and maintain a Software Escrow account in the form of a letter from an escrow agent or other acceptable third party.

d. Explain in detail the build environment needed to support and/or compile the source code in the Software Escrow Account.

## 12. ASP Redundancy and Downtime

a. Explain in detail your company's ability to provide 99.99% uptime for remote customer access to the system. Describe the methodology and application/hosting architecture used to ensure this level of reliability.

b. Explain in detail the process used to notify customers of application downtime for both planned and unplanned outages.

c. Explain in detail any geographic separation of redundant datacenters used to mitigate wide area disasters or events.

d. Explain and describe in detail the features used to ensure the security, redundancy, resiliency and integrity of the datacenter(s) hosting the application, infrastructure and other components.

# APPENDIX B1
## FUNCTIONALITY AND INTEGRATION RESPONSE FORM FOR A COUNTY HOSTED SOLUTION

The functionality and integration requirements of the RFP are listed in this section. Offeror, if proposing more than one type of solution, please submit a Functionality and Integration form for each solution.

# APPENDIX B2
## FUNCTIONALITY AND INTEGRATION RESPONSE FORM FOR AN ASP (VENDOR HOSTED) SOLUTION

The functionality and integration requirements of the RFP are listed in this section. Offeror, if proposing more than one type of solution, please submit a Functionality and Integration form for each solution.

Appendices B1 and B2 are provided in editable Excel format. Reference Section III.B, Response Format and Organization, Original and Copies, Offerors must include the completed Excel worksheets for Appendices B1 and/or B2. These are to be contained in the two (2) identical CDs submitted. The CDs are to include the electronic copies of the **complete proposal** created in Microsoft Office (Word, Excel, and/or Project).

NOTE: Requirements listed on Appendix B1/B2 are *not* mandatory, unless specifically marked as such. Systems not meeting these requirements *will not be* automatically disqualified.

# APPENDIX C1

# IMPLEMENTATION, PROJECT MANAGEMENT, TRAINING, AND ONGOING SUPPORT FOR A COUNTY HOSTED SOLUTION

****** If proposing a county hosted solution, please also review Attachment 4, VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS for reference. Attachment 4 does not have to be submitted at the time of proposal submission. However, Offeror must submit a completed form when requested by the County.*

## 1. Project Implementation Plan and Project Management Team

a. Include the implementation plan the Offeror intends to employ for the project and an explanation of how it will support the project requirements and logically lead to the required deliverables. The description shall include the organization of the project team, including accountability and lines of authority.

b. Describe services to be provided to ensure success of the project e.g. publicize the system to employees, organizing support infrastructure and processes, consulting on content set up and management etc.

c. Describe how the relationship between the County and Offeror will be managed from an account and technical support perspective.

d. Describe what is required of the County to ensure the successful implementation of the system.

e. Include the steps that will be undertaken to identify and resolve any issues or problems before, during and after the implementation.

f. Include a list of proposed project staff and key personnel.

g. Provide resumes, experience narratives and at least one reference for key personnel who will be assigned to the project, if awarded the contract.

h. Explain the relationship of the project management team with the Offeror, including job title and years of employment with the Offeror; role to be played in connection with the proposal; relevant certifications and experience.

## 2. Statement of Work (SOW) - Training Plan

a. Include a description for training of both real time and batch responses for three different audiences:

i. Power users/administrators, general users, Content creators and Instructors.
ii. Technical administrators of the proposed system.
iii. Technical operations staff and support staff for the proposed system.

b. Describe the type and quantity of training that will be provided for each audience. The description must include:

   i. The methods by which training will be provided e.g. online, on-site, webcast, self-paced online courses etc.;
   ii. A recommended training curriculum;
   iii. Explain how the Offeror will work with the County to determine training needs and tailor the curriculum;
   iv. Explain the type of training that will be provided at what stage/phase of the project as well as follow-up training after implementation;
   v. Explain the ability to provide training at a County location.

c. Describe the training facility requirements for physical layout, communication needs (internet connectivity, etc.), projectors, # of computers, etc. that are needed to fulfill the proposed training plan. Identify which elements of the training facility will be supplied by the Offeror.

## 3. SOW - Project Work Plan

Include a detailed work plan for the implementation and operation of the proposed system.

a. **Task Level -**The plan shall include all activities necessary for a successful project down to the task level. No task can exceed more than eighty hours in the work plan.

b. **Identify All Resources -** The plan shall clearly identify all Offeror (including subcontractors) and using agency resources required to successfully complete the project. Provide job descriptions and the number of personnel to be assigned to tasks supporting implementation of the project. Identify County resources needed for each task.

c. **Deliverables** – describe the deliverables of each task.

d. **Time lines** – describe the timeline of each task.

e. **Acceptance criteria** – describe the criteria used to determine completion of each task.

f. **Plan Progress Charts -** The plan shall include appropriate progress/Gantt charts that reflect the proposed schedule and all major milestones. A sample project plan shall be submitted using Microsoft Project.

## 4. System Documentation

a. Describe the documentation provided to facilitate system implementation.

b. Describe the System Administrator documentation provided.

c. Describe if user groups exist to collaborate on issues pertaining to the Offeror’s software, including how often and where they meet. Explain if the user group is a separate independent organization or funded and organized by the Offeror.

d. Attach a listing summarizing available stock (“canned”) reports provided by the solution and a sample of each.

e. Describe how system documentation is provided (online, hard copy etc.) for the initial implementation as well as future updates and releases.

## 5. Acceptance Test Plan

Include an acceptance test plan. The plan shall individually address each system component that comprises of the proposed system, approach for load testing, and number of people to be involved in testing. The plan should document the acceptance testing approach, resources and/or tools that may be used to validate the functions and features of the proposed system. Include an example test plan that is representative of the structure, content, and level of detail planned for this project.

## 6. Risk Management

Submit a risk assessment using the methodology published by the Project Management Institute or other comparable methodology. Include risk mitigation strategies as well as the resources the using agency may utilize to reduce risk.

## 7. On-Going Service and Support

a. Describe the post implementation follow-up activities that will be provided by the Offeror, specifically addressing the following tasks:

   i. Post-live system debugging to bring application into full conformance with documentation, proposal and modification specifications
   ii. Six-month and 12-month post live operational (non-technical) audits to review utilization of the software and to provide recommendations for optimizing benefits.
   iii. Describe how application and support documentation is updated and distributed.

b. Provide the normal hours and describe the channels (phone, email, web, etc.) for support. Describe how after hours support is provided. Describe the support and escalation process, including response times.

c. Indicate the current version of the package. Indicate when the next major version of the package will be available. For major software upgrades, describe how often upgrades are released, how upgrades are defined, developed, tested and released, how customers are notified and educated about the upgrade. Describe the decision process on how new features and functions get included in the product.

d. Explain if the cost of upgrades (including “patches”, corrections to defects, feature enhancements, and minor and major version updates) is included with the proposed solution.

e. Explain if software upgrades, or other maintenance window, will impose a service disruption on the system. If yes, discuss frequency and duration of the service disruptions.

f. Explain if there is a user group. If yes, explain how often they meet and where the meetings are held. Include if the user group is a separate independent organization or funded and organized by the Offeror.

## 8. Value Added Services (Optional)

Offerors are encouraged but not required to propose any optional value added services they believe would help the using agency to effectively implement, operate or use the proposed system. Information provided in this section must be directly relevant to emergency notification systems and not exceed two (2) pages in length.

# APPENDIX C2
## IMPLEMENTATION, PROJECT MANAGEMENT, TRAINING, AND ONGOING SUPPORT FOR AN ASP (VENDOR HOSTED) SOLUTION

**** If proposing an ASP solution, please submit Appendix G, ASP SECURITY ASSESSMENT CHECKLIST, with your proposal.*

### 1. Project Implementation Plan and Project Management Team

a. Include the implementation plan the Offeror intends to employ for the project and an explanation of how it will support the project requirements and logically lead to the required deliverables. The description shall include the organization of the project team, including accountability and lines of authority.

b. Describe services to be provided to ensure success of the project e.g. publicize the system to employees, organizing support infrastructure and processes, consulting on content set up and management etc.

c. Describe how the relationship between the County and Offeror will be managed from an account and technical support perspective.

d. Describe what is required of the County to ensure the successful implementation of the system.

e. Include the steps that will be undertaken to identify and resolve any issues or problems before, during and after the implementation.

f. Include a list of proposed project staff and key personnel.

g. Provide resumes, experience narratives and at least one reference for key personnel who will be assigned to the project, if awarded the contract.

h. Explain the relationship of the project management team with the Offeror, including job title and years of employment with the Offeror; role to be played in connection with the proposal; relevant certifications and experience.

### 2. Statement of Work (SOW) - Training Plan

a. Include a description for training of both real time and batch responses for three different audiences:

i. Power users/administrators, general users, Content creators and Instructors.
ii. Technical administrators of the proposed system.
iii. Technical operations staff and support staff for the proposed system.

b. Describe the type and quantity of training that will be provided for each audience. The description must include:

i. The methods by which training will be provided e.g. online, on-site, webcast, self-paced online courses etc.;
ii. A recommended training curriculum;
iii. Explain how the Offeror will work with the County to determine training needs and tailor the curriculum;

iv. Explain the type of training that will be provided at what stage/phase of the project as well as follow-up training after implementation;
v. Explain the ability to provide training at a County location.

c. Describe the training facility requirements for physical layout, communication needs (internet connectivity, etc.), projectors, # of computers, etc. that are needed to fulfill the proposed training plan. Identify which elements of the training facility will be supplied by the Offeror.

## 3. SOW - Project Work Plan

Include a detailed work plan for the implementation and operation of the proposed system.

a. **Task Level -**The plan shall include all activities necessary for a successful project down to the task level. No task can exceed more than eighty hours in the work plan.

b. **Identify All Resources -** The plan shall clearly identify all Offeror (including subcontractors) and using agency resources required to successfully complete the project. Provide job descriptions and the number of personnel to be assigned to tasks supporting implementation of the project. Identify County resources needed for each task.

c. **Deliverables** – describe the deliverables of each task.

d. **Time lines** – describe the timeline of each task.

e. **Acceptance criteria** – describe the criteria used to determine completion of each task.

f. **Plan Progress Charts -** The plan shall include appropriate progress/Gantt charts that reflect the proposed schedule and all major milestones. A sample project plan shall be submitted using Microsoft Project.

## 4. System Documentation

a. Describe the documentation provided to facilitate system implementation.

b. Describe the System Administrator documentation provided.

c. Describe if user groups exist to collaborate on issues pertaining to the Offeror’s software, including how often and where they meet. Explain if the user group is a separate independent organization or funded and organized by the Offeror.

d. Attach a listing summarizing available stock (“canned”) reports provided by the solution and a sample of each.

e. Describe how system documentation is provided (online, hard copy etc.) for the initial implementation as well as future updates and releases.

## 5. Acceptance Test Plan

Include an acceptance test plan. The plan shall individually address each system component that comprises of the proposed system, approach for load testing, and number of people to be involved in testing. The plan should document the acceptance testing approach, resources and/or tools that may be used to validate the functions and features of the proposed system. Include an example test plan that is representative of the structure, content, and level of detail planned for this project.

## 6. Risk Management

Submit a risk assessment using the methodology published by the Project Management Institute or other comparable methodology. Include risk mitigation strategies as well as the resources the using agency may utilize to reduce risk.

## 7. On-Going Service and Support

a. Describe the post implementation follow-up activities that will be provided by the Offeror, specifically addressing the following tasks:

   i. Post-live system debugging to bring application into full conformance with documentation, proposal and modification specifications
   ii. Six-month and 12-month post live operational (non-technical) audits to review utilization of the software and to provide recommendations for optimizing benefits.
   iii. Describe how application and support documentation is updated and distributed.

b. Provide the normal hours and describe the channels (phone, email, web, etc.) for support. Describe how after hours support is provided. Describe the support and escalation process, including response times.

c. Indicate the current version of the package. Indicate when the next major version of the package will be available. For major software upgrades, describe how often upgrades are released, how upgrades are defined, developed, tested and released, how customers are notified and educated about the upgrade. Describe the decision process on how new features and functions get included in the product.

d. Explain if the cost of upgrades is included in the annual hosting fee.

e. Explain if software upgrades, or other maintenance window, will impose a service disruption on the system. If yes, discuss frequency and duration of the service disruptions.

f. Explain if there is a user group. If yes, explain how often they meet and where the meetings are held. Include if the user group is a separate independent organization or funded and organized by the Offeror.

## 8. Value Added Services (Optional)

Offerors are encouraged but not required to propose any optional value added services they believe would help the using agency to effectively implement, operate or use the proposed system. Information provided in this section must be directly relevant to emergency notification systems and not exceed two (2) pages in length.

# APPENDIX D1
# PROPOSAL COST RESPONSE FORM FOR A COUNTY HOSTED SOLUTION

***Offeror*** – please complete the applicable sections based upon your proposed solution. If proposing both types of solutions, you must complete one cost response form for each solution. The proposed cost shall include all fees, including one-time and recurring, sales tax and value added options. Indicate if items are taxable or non-taxable.

All pricing proposals must be submitted using the form as provided here in Appendix D1. **I**n addition, Offerors may submit their own pricing structure/format for further clarity.

Offeror Name: ___________________________________

## Section I – One Time Costs

| DESCRIPTION | PROPOSED PRICE |
|---|---|
| 1. Proposed Software | |
| 2. Customization | |
| 3. Installation/Implementation | |
| 4. Project Management | |
| 5. Training, including all materials | |
| 6. Travel Expenses<br>(Total from Section II below) | |
| 7. Other One-time Costs<br>(Total from Section III below) | |
| 8. Applicable Sales Tax | |
| **Total One Time Cost** | |

## Section II – Travel Expenses

Please itemize the travel expense in Row 6 in the above table, if any.

Description Cost

1. _______________________________________________ $__________________

Appendix D1
PROPOSAL COST RESPONSE FORM
FOR A COUNTY HOSTED SOLUTION

2. ______________________________ $______________

3. ______________________________ $______________

4. ______________________________ $______________

Total $ ______________

## Section III – Other One-time Costs

*Please itemize all other costs, including, but not limited to: enhancement at an additional cost, proposed modules, third party software to operate the proposed software, etc. Use an attachment, if necessary. Be sure to state the total in Row 7 in the above table.

Description Cost

1. ______________________________ $______________

2. ______________________________ $______________

3. ______________________________ $______________

Total $ ______________

## Section IV – Recurring Annual Costs

List any recurring cost below.

| MAINTENANCE AND SUPPORT | LIST PRICE/COST | PROPOSED COST | DISCOUNT % OFF LIST PRICE/COST |
|---|---|---|---|
| 1. Year One | | | |
| 2. Year Two | | | |
| 3. Year Three | | | |
| 4. Year Four | | | |
| 5. Year Five | | | |
| **TOTAL** | | | |

OFFEROR NAME: ______________________________

Appendix D1
PROPOSAL COST RESPONSE FORM
FOR A COUNTY HOSTED SOLUTION

| ESCROW ACCOUNT | ANNUAL FEE |
|---|---|
| 1. Year One | |
| 2. Year Two | |
| 3. Year Three | |
| 4. Year Four | |
| 5. Year Five | |
| **TOTAL** | |

## Section V – Other Value Added Services:

Please itemize other value added services cost below.

Description Cost ___

1. ________________________________ $__________

2. ________________________________ $__________

OFFEROR NAME: ________________________________

# APPENDIX D2
# PROPOSAL COST RESPONSE FORM FOR AN ASP (VENDOR HOSTED) SOLUTION

Offeror – please complete the applicable sections based upon your proposed solution. If proposing both types of solutions, you must complete one cost response form for each solution. The proposed cost shall include all fees, including one-time and recurring, sales tax, and value added options. Indicate if items are taxable or non-taxable.

All pricing proposals must be submitted using the form as provided here in Appendix D2. ***In addition***, Offerors may submit their own pricing structure/format for further clarity.

Offeror Name: ________________________________

## Section I – One Time Costs

| DESCRIPTION | PROPOSED PRICE |
|---|---|
| 1. Proposed Software | |
| 2. Customization | |
| 3. Installation/Implementation | |
| 4. Project Management | |
| 5. Training, including all materials | |
| 6. Travel Expenses<br>(Total from Section II below) | |
| 7. Other One-time Costs<br>(Total from Section III below) | |
| 8. Applicable Sales Tax | |
| **Total One Time Cost** | |

## Section II – Travel Expenses

Please itemize the travel expense in Row 6 in the above table, if any.

Description Cost

1. ________________________________ $__________

2. ________________________________ $__________

Appendix D2
PROPOSAL COST RESPONSE FORM
FOR AN ASP (VENDOR HOSTED) SOLUTION

3. ______________________________________________ $_________________

4. ______________________________________________ $_________________

Total $ ________________

## Section III – Other One-time Costs

*Please itemize all other costs, including, but not limited to: enhancement at an additional cost, proposed modules, third party software to operate the proposed software, etc. Use an attachment, if necessary. Be sure to state the total in Row 7 in the above table.

Description Cost

1. ______________________________________________ $_________________

2. ______________________________________________ $_________________

3. ______________________________________________ $_________________

Total $ ________________

## Section IV – Recurring Annual Costs

List any recurring cost below.

| **HOSTING FEE** | **LIST PRICE/COST** | **PROPOSED COST** | **DISCOUNT % OFF LIST PRICE/COST** |
|---|---|---|---|
| 1. Year One | | | |
| 2. Year Two | | | |
| 3. Year Three | | | |
| 4. Year Four | | | |
| 5. Year Five | | | |
| **TOTAL** | | | |

OFFEROR NAME: ____________________________________________________

Appendix D2
PROPOSAL COST RESPONSE FORM
FOR AN ASP (VENDOR HOSTED) SOLUTION

## T1 (*If applicable*)

| DESCRIPTION | PROPOSED COST |
|---|---|
| 1. Set Up Fees | |
| 2. Monthly maintenance fees | |
| 3. Other | |

## Section V – Other Value Added Services:

Please itemize other value added services cost below.

Description Cost

1. ________________________________ $______________

2. ________________________________ $______________

OFFEROR NAME: ________________________________________

# APPENDIX E
# NON-COLLUSION DECLARATION

I, ____________________________________________________________, am the
(Print Name)
_____________________________________ of _________________________________,
(Position/Title) (Name of Company)

the party making the foregoing proposal that the proposal is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the bid is genuine and not collusive or sham; that the Offeror has not directly or indirectly induced or solicited any other Offeror to put in a false or sham bid; and has not directly or indirectly colluded, conspired, connived, or agreed with any Offeror or anyone else to put in a sham bid, or that anyone shall refrain from bidding; that the Offeror has not in any manner directly or indirectly, sought by agreement, communication, or conference with anyone to fix the bid price of the Offeror or any other Offeror, or to fix any overhead, profit, or cost element of the bid price, or of that of any other Offeror, or to secure any advantage against the public body awarding the contract of anyone interested in the proposed contract; that all statements contained in the bid are true; and, further, that the Offeror has not, directly or indirectly, submitted his or her bid price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company association, organization, bid depository, or to any member or agent thereof to effectuate a collusive or sham bid.

I declare under penalty of perjury under the Laws of the State of California that the foregoing is true and correct:

COMPANY NAME: ________________________________________________

AUTHORIZED
SIGNATURE _____________________________________________________

PRINT NAME: ____________________________________________________

DATE: _________________________________________________________

# APPENDIX F - DECLARATION OF LOCAL BUSINESS

Santa Clara County gives local businesses a preference in formal solicitations of goods and services as set forth in the Board Policy, Section 5.3.13. A bidder or proposer has the option of qualifying for the preference by self-declaring its qualification as a “local business.” By signing below, the bidder or proposer is certifying its qualification as a “local business” for purposes of application of Santa Clara County’s policy and is deemed to be applying for the local preference.

All information submitted is subject to investigation, as well as to disclosure to third parties under the California Public Records Act. Incomplete, unclear, or incomprehensible responses to the following will result in the bid or proposal not being considered for application of Santa Clara County’s local preference policy. False or dishonest responses will result in rejection of the bid or proposal and curtail the firm or individual’s ability to conduct business with the County in the future. It may also result in legal action.

Provide the complete physical address of your business with meaningful “production capability” located within the boundary of the County of Santa Clara. The term “production capability” means sales, marketing, manufacturing, servicing, or research and development capability that substantially and directly enhances the firm’s/bidder’s/proposer’s ability to perform the proposed contract. Post Office box numbers and/or residential addresses may not be used as the sole bases for establishing status as a “Local Business.” If you have more than one physical address in Santa Clara County, please provide an attachment with all of the addresses in the form specified below.

Business Name: ____________________________________________________________
Street: ____________________________________________________________________
City/State: ______________________________________ Zip Code: __________________

Please Indicate Business Organization (Check One)

□ Individual Proprietorship □ Corporation

□ Partnership □ Other

By filling this form, bidder/proposer declares its qualification as a local business as defined in County of Santa Clara Board Policy, Section 5.3.13.

The undersigned declares that he or she is an official/agent of responding firm or individual and is empowered to represent, bind, and execute contracts on behalf of the firm or individual.

The undersigned declares under penalty of perjury, under the laws of the State of California, that all statements in this Exhibit and response are true and correct, with full knowledge that all statements are subject to investigation and that any incomplete, unclear, false or dishonest response may be grounds for denial or revocation of the accompanying bid or proposal and may result in being barred from doing business with Santa Clara County as well as additional legal consequences.

______________________________________ ______________________________________
Signature Title

______________________________________ ______________________________________
Name Date

______________________________________
Business License Number (if applicable)

# APPENDIX G – ASP SECURITY ASSESSMENT CHECKLIST

## 1. Application Name: ______________________ Vendor Name:_________________________

Briefly describe the purpose of the application. Include an overview of the application architecture, and identify the data that will be 1) stored on the application server at the Vendor site, and 2) that will be transmitted between the application and the County. Also include information on the user authentication process.

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate This Risk*** | ***Comments*** |
|---|---|---|---|---|
| 16.3.4 | The Vendor has a written Disaster Recovery Plan that offers a viable approach to restoring operations following an emergency situation. | | | |
| 16.3.4a | The Vendor site has adequate, redundant physical and/or logical network connectivity to ensure continued operations following a network failure. | | | |

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| 16.3.4b | The Vendor performs system/application database backups on a schedule that is consistent with the importance of the application. | | | |
| 16.3.4b | Backup media are treated with a level of security commensurate with the classification level of the data they contain. | | | |
| 16.3.4c | Vendor servers are closely monitored for both performance and availability. | | | |
| 16.3.4d | The Vendor is willing to sign a Service level Agreement (SLA) that is consistent with the importance of the application to the County. | | | |
| 16.3.5 | The Vendor has a formal, written Security Policy, and is willing to provide a copy of this policy to the County on request. | | | |
| 16.3.5a | If users access the application directly on the Vendor server, user authentication involves more than a simple User ID/password combination, such as one-time password technology. | | | |

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| 16.3.5b | Once granted access, Users are limited to authorized activities only; i.e., customers are prevented from accessing either applications or data that belong to other customers. | | | |
| 16.3.5c | Vendor network connectivity is protected by firewalls, intrusion detection/ prevention systems, etc. designed to protect against attack. | | | |
| 16.3.5d | The equipment hosting the Department's application is located in a physically secure facility that employs access control measures, such as badges, card key access, or keypad entry systems. | | | |
| 16.3.5d | Vendor servers are kept in locked areas/cages that limit access to authorized personnel. | | | |
| 16.3.5e | Vendor staff is bonded, and/or have been subjected to background checks. | | | |

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| 16.3.5f | Vendor servers are hardened against attack and operating system and security-related software patches are applied regularly. | | | |
| 16.3.5f | Commercially available anti-virus software is used on the servers, and is maintained in a current state with all updates. | | | |
| 16.3.5g | Vendor servers are monitored on a continuous basis, and logs are kept of all activity. | | | |
| 16.3.5g,<br>16.3.5h,<br>16.3.5i | The Vendor is willing to report security breaches and/or security issues to the County. | | | |
| 16.3.5h | The Vendor conducts regular vulnerability assessments, using viable third-party organizations, designed to assess both the Vendor's network infrastructure and the individual servers that host applications. | | | |
| 16.3.5h | The Vendor implements "fixes" to correct vulnerabilities discovered during security audits. | | | |

| ***County***<br><br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| 16.3.5i | The Vendor has a formal, written Incident Response Plan. | | | |
| N/A | (Desirable) The network infrastructure hosting the Department application is “air-gapped” from any other network or customer that the Vendor may have. This means that in an ideal situation, the application environment used by the County uses a separate, dedicated server and a separate network infrastructure. | | | |
| N/A | Identify the APIs that may be part of the solution, and indicate industry standards or best practices employed to ensure security of the data and the integration (e.g., web services, directory services, XML, scripting, etc.) | | | |
| N/A | What application security standards, if any, are followed? (e.g., OASIS, WC3, etc.). | | | |

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| N/A | If the application processes credit card information, has the application been certified as PCI compliant? Include information on the level of compliance (e.g., Merchant Level 2) and how the application has been certified. | | | |
| Policy 13.0, Encryption | Data “in motion,” including user authentication information and credentials, are encrypted. | | | |
| Policy 13.0, Encryption | Data “at rest” (stored on the application server), including user authentication information and credentials, are encrypted. | | | |
| Policy 13.0, Encryption | Encryption or hashing algorithms utilized by the Vendor application infrastructure use standard algorithms that have been published and evaluated by the general cryptographic community. | | | |
| N/A | The Vendor is willing to permit on-site visits by County staff in order to evaluate security measures in place. | | | |

| ***County***<br>***Policy Ref. #*** | ***Description of County Requirement*** | ***Details on How Vendor Meets Requirement*** | ***Other Security Measures That Mitigate Risk*** | ***Comments*** |
|---|---|---|---|---|
| N/A | If the Vendor will be connecting to the County via a private connection (such as a dedicated T1 circuit), the Vendor agrees that the circuit will terminate on the County's extranet, and operation of the circuit will fall within the policies related to network connections from non-County entities. | | | |
| N/A | If access to the application uses the Internet, data traffic between the County and the Vendor is protected through the implementation of SSL-VPN or equivalent technology. | | | |

**County CIO's Office Approval:** ________________________________

**Title:** ________________________________________________

**Date:** ________________________________________________

# APPENDIX H
# OFFEROR'S TERMS AND CONDITIONS

Refer to Section V, Requirements and Offeror Submittal, Item F.4, Other Submittals – Offeror's Terms and Conditions.

# ATTACHMENT 1

## COUNTY OF SANTA CLARA STANDARD TERMS AND CONDITIONS

This Agreement is entered into and is effective ____________ 2012, between the County of Santa Clara, (hereafter referred to as “County”) and __________________ (hereafter referred to as “Contractor”), to provide ________________________ (hereafter referred to as “_____”) with Contractor including all related services and maintenance. It is mutually agreed between the parties:

**1. APPENDICES**

The following Appendices are attached hereto and incorporated herein by reference:

1.1 Appendix A – Price Summary and Compensation Plan

1.2 Appendix B – Statement of Work

1.3 Appendix C – Additional Terms and Conditions [subject matter specific]

1.4 Appendix D – Insurance Requirements

1.5 Appendix E – Software Escrow Agreement

1.7 Appendix F – County Travel Policy

**2. DEFINITIONS**

2.1 “Acceptance Tests" means those tests performed during the Performance Period which are intended to determine compliance of Equipment and Software with the specifications and all other Attachments incorporated herein by reference and to determine the reliability of the Equipment.

2.2 "Application Program" means a computer program which is intended to be executed for the purpose of performing useful work for the user of the information being processed. Application programs are developed or otherwise acquired by the user of the Hardware/Software system, but they may be supplied by the Contractor.

2.3 "Attachment" means a mechanical, electrical, or electronic interconnection to the Contractor-supplied Machine or System of Equipment, manufactured by other than the original Equipment manufacturer that is not connected by the Contractor.

2.4 “Commercial Software” means Software developed or regularly used that: (i) has been sold, leased, or licensed to the general public; (ii) has been offered for sale, lease, or license to the general public; (iii) has not been offered, sold, leased, or licensed to the public but will be available for commercial sale, lease, or license in time to satisfy the delivery requirements of this Agreement; or (iv) satisfies a criterion expressed in (i), (ii), or (iii) above and would require only minor modifications to meet the requirements of this Agreement.

2.5 “County Data” shall mean shall mean data and information received by Contractor from County. County shall remain the owner of County Data.

2.6 “Custom Software” means Software that does not meet the definition of Commercial Software.

2.7 "Data Processing Subsystem" means a complement of Contractor-furnished individual Machines, including the necessary controlling elements (or the functional equivalent) and Operating Software, if any, which are acquired to operate as an integrated group, and which are interconnected entirely by Contractor-supplied power and/or signal cables; e.g., direct access controller and drives, a cluster of terminals with their controller, etc.

2.8 "Data Processing System (System)" means the total complement of Contractor-furnished Machines, including one or more central processors (or instruction processors) and Operating Software, which are acquired to operate as an integrated group.

2.9 “Deliverables” means Goods, Software, Information Technology, telecommunications technology, and other items (e.g. reports) to be delivered pursuant to this Agreement, including any such items furnished incident to the provision of services.

2.10 "Designated CPU(s)" means for each product, if applicable, the central processing unit of the computers or the server unit, including any associated peripheral units. If no specific “Designated CPU(s)” are specified on the Agreement, the term shall mean any and all CPUs located at the site specified therein.

2.11 "Documentation" means nonproprietary manuals and other printed materials necessary or useful to the County in its use or maintenance of the Equipment or Software provided hereunder. Manuals and other printed materials customized for the County hereunder constitute Documentation only to the extent that such materials are described in or required by the Statement of Work (“SOW”).

2.12 "Equipment" is an all-inclusive term which refers either to individual Machines or to a complete Data Processing System or subsystem, including its Hardware and Operating Software (if any).

2.13 "Equipment Failure" is a malfunction in the Equipment, excluding all external factors, which prevents the accomplishment of the Equipment’s intended function(s). If microcode or Operating Software residing in the Equipment is necessary for the proper operation of the Equipment, a failure of such microcode or Operating Software which prevents the accomplishment of the Equipment’s intended functions shall be deemed to be an Equipment Failure.

2.14 "Facility Readiness Date" means the date specified in the SOW by which the County must have the site prepared and available for Equipment delivery and installation.

2.15 “Goods” means all types of tangible personal property, including but not limited to materials, supplies, and Equipment (including computer and telecommunications Equipment).

2.16 "Hardware" usually refers to computer Equipment and is contrasted with Software. See also Equipment.

2.17 "Installation Date" means the date specified in the SOW by which the Contractor must have the ordered Equipment ready (certified) for use by the County.

2.18 "Information Technology" includes, but is not limited to, all electronic technology systems and services, automated information handling, System design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications which include voice, video, and data communications, requisite System controls, simulation, electronic commerce, and all related interactions between people and Machines.

2.19 “Licensed Software” is the computer software in object code format, along with Documentation that is provided to County pursuant to this Agreement.

2.20 "Machine" means an individual unit of a Data Processing System or subsystem, separately identified by a type and/or model number, comprised of but not limited to mechanical, electro-mechanical, and electronic parts, microcode, and special features installed thereon and including any necessary Software, e.g., central processing unit, memory module, tape unit, card reader, etc.

2.21 "Machine Alteration" means any change to a Contractor-supplied Machine which is not made by the Contractor, and which results in the Machine deviating from its physical, mechanical, electrical, or electronic (including microcode) design, whether or not additional devices or parts are employed in making such change.

2.22 "Maintenance Diagnostic Routines" means the diagnostic programs customarily used by the Contractor to test Equipment for proper functioning and reliability.

2.23 “Manufacturing Materials” means parts, tools, dies, jigs, fixtures, plans, drawings, and information produced or acquired, or rights acquired, specifically to fulfill obligations set forth herein.

2.24 "Mean Time Between Failure (MTBF)" means the average expected or observed time between consecutive failures in a System or component.

2.25 "Mean Time to Repair (MTTR)" means the average expected or observed time required to repair a System or component and return it to normal operation.

2.26 "Operating Software" means those routines, whether or not identified as Program Products, that reside in the Equipment and are required for the Equipment to perform its intended function(s), and which interface the operator, other Contractor-supplied programs, and user programs to the Equipment.

2.27 "Operational Use Time" means for performance measurement purposes that time during which Equipment is in actual operation by the County. For maintenance Operational Use Time purposes, that time during which Equipment is in actual operation and is not synonymous with power on time.

2.28 "Performance Testing Period" means a period of time during which the County, by appropriate tests and production runs, evaluates the performance of newly installed Equipment and Software prior to its acceptance by the County.

2.29 "Period of Maintenance Coverage" means the period of time, as selected by the County, during which maintenance services are provided by the Contractor for a fixed monthly charge, as opposed to an hourly charge for services rendered. The Period of Maintenance Coverage consists of the Principal Period of Maintenance and any additional hours of coverage per day, and/or increased coverage for weekends and holidays.

2.30 "Preventive Maintenance" means that maintenance, performed on a scheduled basis by the Contractor, which is designed to keep the Equipment in proper operating condition.

2.31 "Principal Period of Maintenance" means any nine consecutive hours per day (usually between the hours of 7:00 a.m. and 6:00 p.m.) as selected by the County, including an official meal period not to exceed one hour, Monday through Friday, excluding holidays observed at the installation.

2.32 "Programming Aids" means Contractor-supplied programs and routines executable on the Contractor's Equipment which assists a programmer in the development of applications including language processors, sorts, communications modules, data base management systems, and utility routines, (tape-to-disk routines, disk-to-print routines, etc.).

2.33 "Program Product" means programs, routines, subroutines, and related items which are proprietary to the Contractor and which are licensed to the County for its use, usually on the basis of separately stated charges and appropriate contractual provisions.

2.34 "Remedial Maintenance" means that maintenance performed by the Contractor which results from Equipment (including Operating Software) failure, and which is performed as required, i.e., on an unscheduled basis.

2.35 "Site License" means for each product, the term "Site License" shall mean the license established upon acquisition of the applicable number of copies of such product and payment of the applicable license fees as set forth in the SOW.

2.36 "Software" means an all-inclusive term which refers to any computer programs, routines, or subroutines supplied by the Contractor, including Operating Software, Programming Aids, Application Programs, and Program Products.

2.37 "Software Failure" means a malfunction in the Contractor-supplied Software, other than Operating Software, which prevents the accomplishment of work, even though the Equipment (including its Operating Software) may still be capable of operating properly. For Operating Software failure, see definition of Equipment Failure.

2.38 "System" means the complete collection of Hardware, Software and services as described in this Agreement, integrated and functioning together, and performing in accordance with this Agreement.

2.39 "U.S. Intellectual Property Rights" means intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, copyrights, and U.S. patents.

## 3. NON-EXCLUSIVE AGREEMENT

This Agreement does not establish an exclusive contract between the County and the Contractor. The County expressly reserves rights to, without limitation, the following: the right to utilize others to provide products, support and services; the right to request proposals from others with or without requesting proposals from the Contractor; and the unrestricted right to bid any such product, support or service.

## 4. TERM

4.1 This Agreement shall not be effective or binding unless approved in writing by the Director of Procurement, or authorized designee, as evidenced by their signature as set forth in this Agreement. The term of the Agreement shall be for three (3) years from the effective date. The County shall have the right to exercise two (2) one-year optional renewals, or one (1) two-year optional renewal.

4.2 Furthermore, at any time during the term of the Agreement, the Agreement is subject to termination pursuant to Section xx 3 of this Agreement. The County may contract with the Contractor for maintenance beyond the term of this Agreement.

4.3 The effective date of this Agreement is _______________, 2012.

## 5. TERMINATION

5.1 Termination for Convenience

5.1.1 The County may terminate this Agreement or any contract release purchase order at any time for the convenience of the County by giving thirty (30) calendar days written notice specifying the effective date and scope of such termination.

5.1.2 In no event shall the County be liable for any loss of profits on the resulting order or portion thereof so terminated.

5.1.3 In the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other materials (collectively referred to as “materials”) prepared by Contractor under this Agreement contract release purchase order shall become the property of the County and shall be promptly delivered to the County. Upon receipt of such materials, County shall pay the Contractor as full compensation for performance, the unit or pro rata price for the then-accepted portion of Deliverables and/or services.

5.1.4 By termination under this paragraph, neither County nor the Contractor may nullify obligations, if any, already incurred for performance or failure to perform prior to the date of termination.

5.1.5 Termination under this paragraph may be made with or without cause.

5.2 Termination for Cause

5.2.1 County may terminate this Agreement or any contract release purchase order, in whole or in part, for cause upon ten (10) calendar days written notice to

Contractor. For purposes of this Agreement, cause includes, but is not limited to, any of the following: (a) material breach of this Agreement or any contract release purchase order by Contractor, (b) violation by Contractor of any applicable laws or regulations; (c) assignment or delegation by Contractor of the rights or duties under this Agreement without the written consent of County or (d) less than perfect tender of delivery or performance by Contractor that is not in strict conformance with terms, conditions, specifications, covenants, representations, warranties or requirements in this Agreement or any contract release purchase order.

5.2.2 In the event of such termination, the Contractor shall be liable for any costs incurred by the County because of Contractor's default. For instance, the County may purchase or obtain Deliverables elsewhere and the defaulting Contractor shall be liable for the difference between Contractor's price pursuant to this Agreement, and all costs incurred by the County. The Contractor shall promptly reimburse the County for the full amount of its liability, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract or contract release purchase order with the County.

5.2.3 If, after notice of termination under the provisions of this clause, it is determined for any reason that the Contractor was not in default under this provisions of this clause, the rights and obligations of the parties shall be the same as if the notice of termination had been issued pursuant to the Termination For Convenience clause.

5.2.4 In lieu of terminating immediately upon contractor's default, County may, at its option, provide written notice specifying the cause for termination and allow Contractor ten (10) calendar days (or other specified time period) to cure. If, within ten (10) calendar days (or other specified time) after the County has given the Contractor such notice, Contractor has not cured to the satisfaction of the County, or if the default cannot be reasonably cured within that time period, County may terminate this Agreement at any time thereafter. County shall determine whether Contractor's actions constitute complete or partial cure. In the event of partial cure, County may, at its option, decide whether to (a) give Contractor additional time to cure while retaining the right to immediately terminate at any point thereafter for cause; or (b) terminate immediately for cause. If County determines that the Contractor's actions contribute to the curtailment of an essential service or pose an immediate threat to life, health or property, County may terminate this Agreement immediately without penalty upon issuing either oral or written notice to the Contractor and without any opportunity to cure.

5.3 Termination for Lack of Appropriation: The term of the Agreement between Contractor and County, and the purchase of Deliverables and/or services hereunder, are contingent on the appropriation of funds by the County. Should sufficient funds not be appropriated, this Agreement may be terminated by County at any time by providing Contractor with thirty (30) calendar days written notice. In the event of such Termination for Lack of Appropriation, County shall be responsible only for any undisputed, unpaid balances for

Deliverables and/or services provided by Contractor and accepted by County prior to the effective date of termination.

5.4 Termination for Bankruptcy: If Contractor is adjudged to be bankrupt or should have a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of Contractor's insolvency, the County may terminate this Agreement immediately without penalty.

5.5 Budgetary Contingency: Performance and/or payment by the County pursuant to this Agreement are contingent upon the appropriation of sufficient funds by the County for services covered by this Agreement. If funding is reduced or deleted by the County for services covered by this Agreement, the County may, at its option and without penalty or liability, terminate this Agreement or offer an amendment to this Agreement indicating the reduced amount.

## 6. NECESSARY ACTS AND FURTHER ASSURANCES

The Contractor shall at its own cost and expense execute and deliver such further documents and instruments and shall take such other actions as may be reasonably required or appropriate to evidence or carry out the intent and purposes of this Agreement.

## 7. COUNTING DAYS

Days are to be counted by excluding the first day and including the last day, unless the last day is a Saturday, a Sunday, or a legal holiday, and then it is to be excluded.

## 8. MODIFICATION

This Agreement or any contract release purchase order may be supplemented, amended, or modified only by the mutual agreement of the parties. No supplement, amendment, or modification of this Agreement contract release purchase order will be binding on County unless it is in writing and signed by County's Director of Procurement, or authorized designee, as evidenced by his/her signature as set forth in this Agreement.

## 9. SCOPE

9.1 Contractor agrees to provide the County all Deliverables and/or services on terms set forth in this Agreement (including Appendices), as well as all necessary equipment and resources. However, this Agreement does not provide authority to ship Deliverables. That authority shall be established by contract release purchase orders placed by the County and sent to Contractor throughout the term of the Agreement. Each and every contract release purchase order shall incorporate all terms of this Agreement and this Agreement shall apply to same.

9.2 The County will consider Contractor to be the single point of contact with regards to all contractual matters, including payment of any and all charges for Deliverables and/or services provided under the Agreement and any issues regarding the subcontractor(s), if any. Contractor shall provide to County quarterly and annual spend and usage reports, at no additional cost.

9.3 Any additional or different terms or qualifications sent by Contractor, including, without limitation, in mailings, attached to invoices or with any Deliverables shipped, shall not become part of the contract between the parties. County's acceptance of Contractor's offer is expressly made conditional on this statement.

9.4 Contractor shall provide to the County, all documentation and manuals relevant to the Deliverables to be supplied, at no additional cost. Contractor shall deliver such documentation either in advance of or concurrently with the delivery of Deliverables.

9.5 Employees and agents of Contractor, shall, while on the premises of the County, comply with all rules and regulations of the premises, including, but not limited to, security requirements.

9.6 Contractor shall be responsible for installation, delivery, training and knowledge transfer activities in relation to the Deliverables being supplied as reasonably required by County and as set forth in the the appendices to this Agreement.

9.7 All equipment shall be delivered to a County site specified in the contract release purchase order, or if not so specified therein, in the SOW/Specifications.

9.8 Unless stated otherwise and agreed to in writing by County, County shall own all Deliverables provided pursuant to this Agreement. County shall also own all modifications and/or enhancements to the Deliverables paid for by County, as well as any and all derivatives created or paid for by County.

9.9 Contractor holds itself out as an expert in the subject matter of the Agreement. Contractor represents itself as being possessed of greater knowledge and skill in this area than the average person. Accordingly, Contractor is under a duty to exercise a skill greater than that of an ordinary person, and the manner in which performance is rendered will be evaluated in light of the Contractor's superior skill. Contractor shall provide equipment and perform work in a professional manner consistent, at minimum, with industry standards.

9.10 Contractor represents that all prices, warranties, benefits and other terms being provided hereunder are fair, reasonable and commensurate with the terms otherwise being offered by Contractor to its current customers ordering comparable Deliverables and/or services.

9.11 County does not guarantee any minimum orders.

9.12 This Agreement shall not be effective or binding unless approved in writing by the County Director of Procurement, or authorized designee, as evidenced by their signature as set forth in this Agreement.

9.13 Furthermore, at any time during the term of the Agreement, the Agreement is subject to termination in accordance with this Agreement. The County may contract with Contractor for recurring services beyond the term of this Agreement and any amendments.

## 10. COST SUMMARY AND COMPENSATION PLAN

10.1 Appendix A of this Agreement is the basis for the pricing and compensation plan. The maximum compensation paid to the Contractor under this Agreement is $______________.

10.2 In the event of a decrease in the cost of recurring fees, Contractor shall extend the lower price(s) to the County and provide prompt written notification to the County. Contractor shall, on an ongoing basis, inform the County of any such special, promotional or reduced pricing.

10.3 In the event that any product on Appendix A is discontinued or upgraded, Contractor shall extend the same contract pricing towards a comparable replacement which is functionally equivalent or upgraded version when available. Minimum mandatory hardware specifications must be included. Unless otherwise stated, prices shall be fixed for the term of the Agreement, including all extensions and/or amendments.

10.4 Additional services, if any, will be billed after services have been rendered.

10.5 Both parties acknowledge that during the term of this Agreement, products and services may be added to the Agreement. In the event that such services are identified, and a cost is associated, the County reserves the right to add the additional services to the Agreement and negotiate cost. The County Contract Administrator will approve the additional work and cost by means of an amendment.

10.6 The County will not pay any cost or charge that is not delineated in this Agreement.

## 11. DISPUTED PAYMENTS

If, due to either an issue with the charges on an invoice or the Contractor's failure to perform its obligations under this Agreement, the County disputes any charge(s) on an invoice, the County may withhold the disputed amount, provided that (a) there is a reasonable basis for the dispute, (b) all other amounts that are not in dispute have been paid in accordance with this Agreement, and (c) the County delivers a written statement to Contractor on or before the due date of the invoice, describing in detail the basis of the dispute and the amount being withheld by the County.

## 12. TIME OF THE ESSENCE

12.1 Time is of the essence in the delivery of Deliverables and/or services by Contractor under this Agreement and any contract release purchase order. In the event that the Contractor fails to deliver Deliverables and/or services on time, the Contractor shall be liable for any costs incurred by the County because of Contractor's delay. For instance, County may purchase or obtain the Deliverables and/or services elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County; or County may terminate on grounds of material and Contractor shall be liable for County's damages.

12.2 The Contractor shall promptly reimburse the County for the full amount of its liability, or, at County's option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

12.3 The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

## 13. DOCUMENTATION

13.1 The Contractor agrees to provide to the County, at no charge, a reasonable number of all nonproprietary manuals and other printed materials, as described within the SOW, and updated versions thereof, which are necessary or useful to the County in its use of the Equipment or Software provided hereunder. The Contractor agrees to provide additional Documentation at prices not in excess of charges made by the Contractor to its other customers for similar Documentation, or if appropriate, to permit County to make copies of same for County's internal use.

13.2 If the Contractor is unable to perform maintenance or the County desires to perform its own maintenance on Equipment purchased under this Agreement then upon written notice by the County the Contractor will provide at Contractor's then current rates and fees adequate and reasonable assistance including relevant Documentation to allow the County to maintain the Equipment based on Contractor's methodology. The Contractor agrees that the County may reproduce such Documentation for its own use in maintaining the Equipment. If the Contractor is unable to perform maintenance, the Contractor agrees to license any other contractor that the County may have hired to maintain the Equipment to use the above noted Documentation. The County agrees to include the Contractor's copyright notice on any such Documentation reproduced, in accordance with copyright instructions to be provided (in writing) by the Contractor.

## 14. SERVICE LEVEL AGREEMENT

14.1 Contractor warrants that the service provided pursuant to this Agreement shall adhere to the service levels and benchmarks specified in the SOW. Unavailability does not mean an inability to connect to the service due to a failure between the County's computer and the Internet. System availability and response time shall be accurately, truthfully and precisely monitored by Contractor on a 24x7x365 basis. Contractor shall provide a system availability and response time report at any time upon request by County.

14.2 This Agreement may be terminated for cause and without penalty if the Contractor fails to meet, for three (3) months in any twelve (12) month period, the service levels and benchmarks specified in the SOW, or experiences any period of total unavailability that has not been cured within three (3) hours to the reasonable satisfaction of the County.

## 15. HAZARDOUS SUBSTANCES

If any product being offered, delivered or supplied to the County is listed in the Hazardous Substances List of the Regulations of the Director of Industrial Relations with the California Occupational Safety and Health Standards Board, or if the product presents a physical or health hazard as defined in the California Code of Regulations, General Industry Safety Order, Section 5194 (“T8CCR”), Hazard Communication, the Contractor must include a Material Safety Data Sheet (“MSDS”) with delivery, or shipment. Each MSDS must reference the contract/purchase order number, and identify the "Ship To Address." All shipments and containers must comply with the labeling requirements of Title 49, Code of Federal Regulations by identifying the hazardous substance, name and address of manufacturer, and appropriate hazard warning regarding potential physical safety and health hazard.

## 16. SHIPPING AND RISK OF LOSS

16.1 Deliverables shall be packaged, marked and otherwise prepared by Contractor in suitable containers in accordance with sound commercial practices. Contractor shall include an itemized packing list with each shipment and with each individual box or package shipped to the County. The packing list shall contain, without limitation, the applicable contract release purchase order number.

16.2 Unless otherwise specified in writing, all shipments by Contractor to County will be F.O.B. point of destination. Freight or handling charges are not billable unless such charges are referenced on the order. Transportation receipts, if required by contract release purchase order, must accompany invoice. Regardless of F.O.B. point, Contractor shall bear all risks of loss, injury, or destruction to Deliverables and materials ordered herein which occur prior to acceptance by County; and such loss, injury or destruction shall not release Contractor from any obligation hereunder.

16.3 Any shipments returned to the Contractor shall be delivered as F.O.B. shipping point.

## 17. INSPECTION, TEST, ACCEPTANCE, REJECTION AND RELATED RIGHTS

Unless otherwise specified in the SOW:

17.1 All Deliverables and/or services are subject to inspection, testing, approval and acceptance by the County. Inspection shall be made within a reasonable time (but in no event longer than sixty (60) calendar days) after delivery. If the Deliverables, services, or the tender of delivery fail in any respect to conform to the Agreement, the County may reject the entire tender, accept the entire tender, or, if the Deliverables are commercially divisible, may, at its option, accept any commercial unit or units and reject the rest.

17.2 Inspection

17.2.1 Contractor and its subcontractors will provide and maintain a quality assurance system acceptable to the County covering Deliverables and/or services under this Contract and will tender to the County only those Deliverables that have been inspected and found to conform to this Agreement’s requirements.

17.2.2 Contractor will keep records evidencing inspections and their result, and will make these records available to the County during performance and for three (3) years after final payment. Contractor shall permit the County to review procedures, practices, processes, and related documents to determine the acceptability of Contractor's quality assurance System or other similar business practices related to performance of the Agreement.

17.2.3 Contractor and its subcontractors shall provide all reasonable facilities for the safety and convenience of inspectors at no additional cost to the County. Contractor shall furnish to inspectors all information and data as may be reasonably required to perform their inspection.

17.2.4 All Deliverables and/or services may be subject to final inspection, test and acceptance by the County at destination, notwithstanding any payment or inspection at source.

17.3 Test

17.3.1 County will use the criteria established in this Agreement, the SOW, or any subsequent sub-SOW to determine the acceptance of each task and to test the Deliverables and/or services.

17.3.2 If the County, in its sole discretion, determines that the Deliverables and/or services have failed to meet a specific task, specification or requirements of the SOW, any sub-SOW, or this Agreement, or that features or functions said to be present in the Contractor's Documentation are absent or do not function properly, County may execute any or all of the following:

(i) Have the Contractor modify the Deliverables and/or services to conform to the Documentation;

(ii) Extend the acceptance testing period for a reasonable time period to allow time for Contractor to remedy the problems; or

(iii) Cancel this Agreement and its obligations to Contractor. Any pre-payments made to the Contractor shall be prorated to the termination date and the remainder refunded to the County.

17.4 Acceptance

17.4.1 Acceptance is set forth in the SOW.

17.5 Rejection

17.5.1 County shall give written notice of rejection of Deliverables delivered and/or services performed during the period set forth in Section 17.1 of this Agreement. Such notice of rejection will state the respects in which the Deliverables and/or services do not substantially conform to their specifications. Acceptance by County will be final and irreversible, except as it relates to latent defects, fraud, and gross mistakes amounting to fraud. Acceptance shall not be construed to waive any warranty rights that the County might have at law or by express reservation in this Agreement with respect to any nonconformity.

17.5.2 Contractor shall be responsible to reclaim and remove any rejected Deliverables and/or items at its own expense. Should Contractor fail to reclaim or remove any rejected Deliverables and/or items within a reasonable time, County shall, at its option dispose of such Deliverables and/or items and require reimbursement from Contractor for any costs or expenses incurred.

17.6 Corrective Action:

17.6.1 Contractor shall comply with all applicable federal state, and local laws and regulations relating to its performance under this Agreement in all material respects.

17.6.2 If County discovers any practice, procedure, or policy of Contractor which materially deviates from the terms or requirements of this Agreement, which violates federal, state or local laws or regulations, the County, in addition to its termination rights, may notify Contractor that corrective action is required.

17.6.3 Contractor shall correct any and all discrepancies, violations, or deficiencies within thirty (30) calendar days, unless the corrective action requires additional time, in which case Contractor shall have a period of time to make corrections.

17.6.4 In the event that the Contractor’s Deliverables and/or services are not accepted by County, the Contractor shall be liable for any costs incurred by the County because of such failure by Contractor. For instance, County may purchase or obtain the Deliverables and/or services elsewhere and the Contractor shall be liable for the difference between the price in the Agreement and the cost to the County, and any other costs incurred; or County may terminate for cause on grounds of material breach and Contractor shall be liable for County’s damages.

17.6.5 Contractor shall promptly reimburse the County for the full amount of its liability, or, at County’s option, the County may offset such liability from any payment due to the Contractor under any contract with the County.

17.6.6 The rights and remedies of County provided herein shall not be exclusive and are in addition to any other rights and remedies provided by law. The acceptance by County of late or partial performance with or without objection or reservation shall not waive the right to claim damage for such breach nor constitute a waiver of the rights or requirements for the complete and timely performance of any obligation remaining to be performed by the Contractor, or of any other claim, right or remedy of the County.

## 18. ADJUSTMENT BY COUNTY

The County reserves the right to waive a variation in specification of Deliverables and/or services supplied by the Contractor. Contractor may request an equitable adjustment of payments to be made by County if County requires a change in the Deliverables and/or services to be delivered. Any claim by the Contractor for resulting adjustment of payment must be asserted within thirty (30) calendar days from the date of receipt by the Contractor of the notification of change required by County; provided however, that the Procurement Director, if he/she decides that the facts justify such action, may receive and act upon any such claim asserted at any time prior to final payment made for Deliverables and/or services supplied by Contractor. Where the cost of property made obsolete or excess as a result of a change is included in the Contractor's claim for adjustment, the Procurement Director shall have the right to prescribe the manner of disposition of such property. Nothing in this clause shall excuse performance by Contractor.

## 19. INVOICING

19.1 Contractor shall invoice according to the pricing Appendix of this Agreement. Invoices shall be sent to the County customer or department referenced in the individual contract release purchase order. Invoices for Deliverables and/or services not specifically listed in the Agreement will not be approved for payment.

19.2 Invoices shall include: Contractor's complete name and remit-to address; invoice date, invoice number, and payment term; County contract number; pricing per the Agreement; applicable taxes; and total cost.

19.3 Contractor and County shall make reasonable efforts to resolve all invoicing disputes within seven (7) calendar days.

## 20. AVAILABILITY OF FUNDING

The County's obligation for payment of any contract beyond the current fiscal year end is contingent upon the availability of funding and upon appropriation for payment to the Contractor. No legal liability on the part of the County shall arise for payment beyond June 30 of the calendar year unless funds are made available for such performance.

## 21. PAYMENT

21.1 Payment shall be due net 30 days from the date of final acceptance by County of the Deliverables and/or services ordered, or net 30 days from the date of approval by County of correct and proper invoices, whichever date is later. Payment is deemed to have been made on the date when the County mails the warrant or initiates the electronic fund transfer.

21.2 Notwithstanding anything to the contrary, County shall not make payments prior to receipt of Deliverables and/or services (i.e. the County will not make "advance payments"). Unless specified in writing in a contract release purchase order, the County will not accept partial delivery with respect to any purchase order. Any acceptance of partial delivery shall not waive any of County's rights.

21.3 Sales tax shall be noted separately on every invoice. Items that are not subject to sales tax shall be clearly identified.

21.4 Contractor shall be responsible for payment of all state and federal taxes assessed on the compensation received under this Agreement and such payment shall be identified under the Contractor's federal and state identification number(s). Contractor shall also be responsible for all state and local property taxes assessed on property that is the subject of this Agreement.

21.5 The County does not pay Federal Excise Taxes (F.E.T). The County will furnish an exemption certificate in lieu of paying F.E.T. Federal registration for such transactions is: County #94-730482K. Contractor shall not charge County for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose, unless expressly authorized by the County.

21.6 Contractor shall be solely responsible for all of Contractor's travel fees and costs. County shall be solely responsible for all of County's travel fees and costs.

## 22. LATE PAYMENT CHARGES OR FEES

The Contractor acknowledges and agrees that the County will not pay late payment charges or fees.

## 23. DISALLOWANCE

In the event the Contractor receives payment for Deliverables and/or services, which payment is later disallowed by the County or state or federal law or regulation, the Contractor shall promptly refund the disallowed amount to the County upon notification. At County's option, the County may offset the amount disallowed from any payment due to the Contractor under any contract with the County.

## 24. DISENTANGLEMENT

24.1 This section shall apply upon termination of this Agreement for any reason.

24.2 Contractor shall cooperate with County and County's other contractors to ensure a smooth transition at the time of termination of this Agreement, regardless of the nature or timing of the termination. Contractor shall cooperate with County's efforts to ensure that there is no interruption of work required under the Agreement and no adverse impact on the supply of Deliverables, provision of services or the County's activities. Contractor shall promptly return to County all County assets or information in Contractor's possession.

24.3 For any software programs developed for use under the County's Agreement, Contractor shall provide a non-exclusive, non-transferable, fully-paid, perpetual, irrevocable, royalty-free worldwide license to the County, at no charge to County, to use, copy, and modify, all work or derivatives that would be needed in order to allow County to continue to perform for itself, or obtain from other providers, the services as the same might exist at the time of termination.

24.4 County shall be entitled to purchase at net book value those Contractor assets used for the provision of services to or for County, other than those assets expressly identified by the parties as not being subject to this provision. Contractor shall promptly remove from County's premises, or the site of the work being performed by Contractor for County, any Contractor assets that County, or its designee, chooses not to purchase under this provision.

24.5 Contractor shall deliver to County or its designee, at County's request, all Documentation and data related to County, including, but not limited to, the County Data and client files, held by Contractor, and after return of same, Contractor shall destroy all copies thereof not turned over to County, all at no charge to County.

## 25. DISPUTES

25.1 The parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute persists, except as otherwise provided in this Agreement, any dispute concerning a question of fact arising under this Agreement that is not disposed of by agreement shall be decided by the Director of Procurement who shall furnish the decision to the Contractor in writing. The decision of the Director of Procurement shall be final and conclusive unless determined by the court of competent jurisdiction to have been fraudulent or capricious, or arbitrary, or so grossly erroneous as necessarily to imply bad faith. The Contractor shall proceed diligently with the performance of the Agreement pending the Director of Procurement’s decision.

25.2 "Disputes" clause does not preclude consideration of legal questions in connection with decisions provided for in paragraph (a) above. Nothing in this Agreement shall be construed as making final the decision of any administrative official, representative, or board on a question of law.

25.3 In the event of a dispute, Contractor shall continue to perform its obligations pursuant to this Agreement for a period not to exceed ninety (90) days from the time that Contractor provides written notice to County of the disputed issue(s).

## 26. ACCOUNTABILITY

Contractors will be the primary point of contact and assume the responsibility of all matters relating to the purchase, including those involving the manufacturer and deliverer or any subcontractor, as well as payment issues. If issues arise, the Contractor must take immediate action to correct or resolve the issues.

## 27. NO ASSIGNMENT, DELEGATION OR SUBCONTRACTING WITHOUT PRIOR WRITTEN CONSENT

27.1 Contractor may not assign any of its rights, delegate any of its duties or subcontract any portion of its work or business under this Agreement or any contract release purchase order without the prior written consent of County. No assignment, delegation or subcontracting will release Contractor from any of its obligations or alter any of its obligations to be performed under the Agreement. Any attempted assignment, delegation or subcontracting in violation of this provision is voidable at the option of the County and constitutes material breach by Contractor. Contractor is responsible for payment to sub-contractors and must monitor, evaluate, and account for the sub-contractor(s) services and operations.

27.2 As used in this provision, "assignment" and "delegation" means any sale, gift, pledge, hypothecation, encumbrance, or other transfer of all or any portion of the rights, obligations, or liabilities in or arising from this Agreement to any person or entity, whether by operation of law or otherwise, and regardless of the legal form of the transaction in which the attempted transfer occurs.

## 28. MERGER AND ACQUISITION

28.1 Neither party may assign this Agreement or transfer any rights to a third party without the prior written consent of the other party, and any such attempt shall be void; provided, however, subject to compliance with the provisions of this Section 28, County shall not unreasonably withhold or delay its consent for Contractor to transfer and/or assign this Agreement to any current wholly owned subsidiary, or pursuant to a corporate plan of merger, reorganization, acquisition or consolidation.

28.2 This Agreement will inure to the benefit of and be binding upon the parties and their respective successors and permitted assigns. The terms of this Agreement will survive an acquisition, merger, divestiture or other transfer of rights or assignment involving Contractor. In the event of an acquisition, merger, divestiture or other transfer of rights, Contractor shall ensure that the acquiring entity or the new entity agrees to be bound by the terms of this Agreement and act in the place of Contractor with respect to all of its obligations as set forth herein. The acquiring entity shall honor all the terms and conditions in this Agreement and (if applicable) provide the functionality of the Deliverables and/or services in a future, separate or renamed product, if the acquiring entity or the new entity reduces or replaces the functionality, or otherwise provide a substantially similar functionality of the Deliverables and/or services at the same pricing levels. No additional license or maintenance fee will apply.

28.3 Contractor shall provide thirty (30) calendar days written notice to the County following the closing of an acquisition, merger, divestiture or other transfer of right involving Contractor.

28.4 Contractor shall provide reasonable assistance to County during the transition period.

## 29. COMPLIANCE WITH ALL LAWS & REGULATIONS

Contractor shall comply with all laws, codes, regulations, rules and orders (collectively, "Regulations") applicable to the Deliverables and/or services to be provided hereunder. Contractor’s violation of this provision shall be deemed a material default by Contractor, giving County a right to terminate the Agreement. Examples of such Regulations include but are not limited to California Occupational Safety and Health Act of 1973, Labor Code §6300 et. seq. the Fair Packaging and Labeling Act, etc. and the standards and regulations issued there under. Contractor shall defend, indemnify and hold the County harmless against any claim, loss, damage, fine, penalty, or any expense whatsoever as a result of Contractor’s failure to comply with the act and any standards or regulations issued there under.

## 30. FORCE MAJEURE

30.1 Neither party shall be liable for failure of performance, nor incur any liability to the other party on account of any loss or damage resulting from any delay or failure to perform all or any part of this Agreement if such delay or failure is caused by events, occurrences, or causes beyond the reasonable control and without negligence of the parties. Such events, occurrences, or causes will include Acts of God/Nature (including fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, riots, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, lockout, blockage, embargo, labor dispute, strike, interruption or failure of electricity or telecommunication service.

30.2 Each party, as applicable, shall give the other party notice of its inability to perform and particulars in reasonable detail of the cause of the inability. Each party must use best efforts to remedy the situation and remove, as soon as practicable, the cause of its inability to perform or comply.

30.3 The party asserting *Force Majeure* as a cause for non-performance shall have the burden of proving that reasonable steps were taken to minimize delay or damages caused by foreseeable events, that all non-excused obligations were substantially fulfilled, and that the other party was timely notified of the likelihood or actual occurrence which would justify such an assertion, so that other prudent precautions could be contemplated.

30.4 The County shall reserve the right to terminate this Agreement and/or any applicable order or contract release purchase order upon non-performance by Contractor. The County shall reserve the right to extend the agreement and time for performance at its discretion.

## 31. CONFLICT OF INTEREST

31.1 Contractor represents and warrants that, to the best of its knowledge, it presently has no interest and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of services required under this Agreement.

31.2 Contractor shall comply, and require its subcontractors to comply, with all applicable (i) professional canons and requirements governing avoidance of impermissible client conflicts applicable to Contractor and such subcontractors; and (ii) federal, state and local conflict of interest laws and regulations applicable to Contractor, such subcontractors and the services, including, without limitation, to the extent applicable, California Government Code section 1090 et. seq., the California Political Reform Act (California Government Code section 87100 et. seq.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 et. seq.). Failure to do so constitutes a material breach of this Agreement and is grounds for termination of this Agreement by the County.

31.3 Contractor shall provide County with the names, description of individual duties to be performed and email addresses of all persons who will be engaged in performance of the agreement, including without limitation colleagues, employees, agents and subcontractors with the exception of those working solely ministerial, secretarial, manual, or clerical capacity. Contractor shall immediately notify the County of the names of individuals working in such a capacity who, during the course of the Agreement, end their service.

31.4 Contractor shall ensure that all individuals identified pursuant to this section understand that they are subject to the Political Reform Act (“PRA”) and shall conform to all requirements of the PRA and other laws and regulations, including, as required, filing of Statements of Economic Interests (Form 700) within thirty (30) calendar days of commencing service pursuant to this Agreement, annually by April 1, and within thirty (30) calendar days of their termination of service pursuant to this Agreement. Form 700 is available on the website of the Fair Political Practices Commission.

### 32. INDEPENDENT CONTRACTOR

Contractor shall supply all Deliverables and/or perform all services pursuant to this Agreement as an independent contractor and not as an officer, agent, servant, or employee of County. Contractor shall be solely responsible for the acts and omissions of its officers, agents, employees, contractors, and subcontractors, if any. Nothing herein shall be considered as creating a partnership or joint venture between the County and Contractor. No person performing any services and/or supplying all Deliverables shall be considered an officer, agent, servant, or employee of County, nor shall any such person be entitled to any benefits available or granted to employees of the County.

### 33. INSURANCE

Contractor shall maintain insurance coverage, throughout the term of this Agreement, pursuant to Appendix ___.

### 34. DAMAGE AND REPAIR BY CONTRACTOR

Any and all damages caused by Contractor's negligence or operations shall be repaired, replaced or reimbursed by Contractor at no charge to the County. Repairs and replacements shall be completed with seventy two (72) hours of the incident unless the County requests or agrees to an extension or another time frame. The clean up of all damage related to accidental or intentional release of any/all non-hazardous or hazardous material (e.g. hydraulic fluid, fuel, grease, etc.) from Contractor's vehicles or during performance shall be responsibility of the Contractor. All materials must be cleaned up in a manner and time acceptable to County (completely and immediately to prevent potential as well as actual environmental damage). Contractor must immediately report each incident to the County's Director of Procurement. Damage observed by Contractor, whether or not resulting from Contractor's operations or negligence shall be promptly reported by Contractor to County. County may, at its option, approve and/or dictate the actions that are in County's best interests.

### 35. LIENS, CLAIMS, AND ENCUMBRANCES AND TITLE

The Contractor represents and warrants that all the Deliverables and/or materials ordered and delivered are free and clear of all liens, claims or encumbrances of any kind. Contractor represents and warrants that it has free and clear title (including any and all intellectual property rights) to the Deliverables and/or materials purchased by County. Title to the Deliverables and/or materials purchased shall pass directly from Contractor to County at the F.O.B. point, subject to the right of County to reject upon inspection.

### 36. CONTRACTOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY

36.1. Contractor shall be liable for damages arising out of injury to the person and/or damage to the property of the County, employees of the County, persons designated by the

County for training, or any other person(s) other than agents or employees of the Contractor, designated by the County for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Contractor's site or at the County's place of business, provided that the injury or damage was caused by the fault or negligence of the Contractor.

36.2 Contractor shall not be liable for damages arising out of or caused by an alteration not made or installed by the Contractor.

## 37. INDEMNITY

Contractor shall defend, indemnify, and hold harmless the County, its officers, agents and employees from any claim, liability, loss, injury or damage arising out of, or in connection with, performance of this Agreement by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for the County. The Contractor shall reimburse the County for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which the Contractor is obligated to defend, indemnify, and hold harmless the County under this Agreement.

## 38. INTELLECTUAL PROPERTY INDEMNITY

Contractor represents and warrants for the benefit of the County and its users that, to its knowledge, as of the effective date of this Agreement, Contractor is the exclusive owner of all rights, title and interest in the Deliverables and/or services provided pursuant to this Agreement. Contractor shall defend, indemnify and hold the County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and reasonable attorneys fees) by a third party alleging the Deliverables and/or services provided pursuant to this Agreement infringe upon any intellectual property rights of third parties.

## 39. LIMITATION OF LIABILITY

39.1 Contractor's liability for damages to the County for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, shall be limited to greater of (i) the insurance limits set forth in Appendix D to this Agreement, or (ii) three (3) times the Purchase Price. For purposes of this Section, "Purchase Price" will mean the aggregate Agreement price as set forth in Section 10 of this Agreement, and any subsequent amendments to this Agreement.

39.2 The foregoing limitation of liability shall not apply to (i) any indemnity or warranty obligation set forth in this Agreement, (ii) Contractor's willful misconduct, gross negligence, or fraud, or (iii) costs or attorney's fees that the County becomes entitled to recover.

39.3 The County's liability for damages for any cause whatsoever, and regardless of the form of action, whether in contract or in tort, shall be limited to the Purchase Price. Nothing herein shall be construed to waive or limit the County's sovereign immunity or any other immunity from suit provided by law.

## 40. WARRANTY

40.1 Any Deliverables and/or services furnished under this Agreement shall be covered by the most favorable commercial warranties that Contractor gives to any of its customers for the same or substantially similar Deliverables and/or services. Any warranties so provided shall supplement, and shall not limit or reduce, any rights afforded to County by any clause in this Agreement, any applicable Uniform Commercial Code warranties, including, without limitation, Implied Warranty of Merchantability and Implied Warranty of Fitness for a Particular Purpose as well as any other express warranty.

40.2 Unless otherwise specified, the warranties in this Section begin upon County's final acceptance of the Deliverables and/or services in question and end one (1) year thereafter. Contractor warrants that:

40.2.1 Deliverables and/or services furnished hereunder shall strictly conform to the requirements of this Agreement (including without limitation all descriptions, specifications, and drawings identified in the SOW) and Contractor's Documentation;

40.2.2 Deliverables shall:

(i) be free from material defects in materials and workmanship;

(ii) be free of illicit or harmful code (i.e. computer viruses, worms, trap doors, time bombs, disabling code, or any similar malicious mechanism designed to interfere with the intended operation of, or cause damage to, computers, data, or Software);

(iii) not contain hidden files or viruses;

(iv) not replicate, transmit or activate themselves;

(v) not alter, damage or erase data or computer programs;

(vi) not contain open source code; and

(vii) not infringe or violate any U.S. Intellectual Property Right.

40.2.3 If the Agreement calls for delivery of Commercial Software, Contractor warrants that such Software will perform in accordance with its license and accompanying Documentation.

40.2.4 All Deliverables supplied shall be new, suitable for the use intended, of the grade and quality specified, free from all defects in design, material and workmanship, in conformance with all samples, drawings, descriptions and specifications furnished by the County, in compliance with all applicable federal, state and local laws and regulations and free of liens, claims and encumbrances.

40.2.5 All Deliverables containing embedded or third party software shall contain a nonexclusive, perpetual, worldwide, and royalty free license to use, reproduce, distribute, demonstrate and prepare derivative works. Should a conflict exist between the terms of any such embedded or third party software license and this Agreement, this Agreement shall take precedence and supersede such other license terms and conditions.  Contractor also represents and warrants that it has all rights to license to County.  Contractor shall pass through all applicable third party warranties to County.

40.2.6  All Deliverables are compatible with County's operating environment.

40.2.7  Contractor shall perform all services in a workmanlike manner and in accordance with Contractor's industry's standards, but in no event less than a reasonable manner.

40.2.8  Security features shall be embedded, enabled and active upon delivery to County, including baseline security configurations for all Deliverables and a defined process to discover and report to County areas within the Deliverables that are vulnerable to security breaches.

40.3 Contractor shall immediately repair and/or replace any Deliverable not conforming to any warranty, or provide services to conform to County's requirements.  If after notice, Contractor fails to repair or replace Deliverables, or to provide services to conform to County's requirements, Contractor shall promptly refund to County the full purchase price paid by the County and the County's Cost to Cover.  This remedy is non-exclusive of other remedies and rights that may be exercised by the County.  Claims for damages may include direct damages, such as cost to repair, as well as incidental and consequential damages.  "Cost to Cover" means the cost, properly mitigated, of procuring Deliverables and/or services of equivalent capability, function, and performance.  Contractor shall also extend the warranty period for the equivalent period of time that the Deliverables are not in conformance with the County's requirements.

40.4 At County's option, Contractor shall use best efforts to repair and/or replace any Deliverable containing open source code or illicit or harmful code.  Contractor shall also extend the warranty period for the equivalent period of time that the Deliverables are not in conformance with the County's requirements.  Contractor shall also extend the warranty period for the equivalent period of time that the Deliverables are not in conformance with the County's requirements.

40.5 If Contractor is unable to repair and/or replace to the County's satisfaction and within a reasonable period of time, County may immediately terminate this Agreement for cause pursuant to section 5 of this Agreement and Contractor shall refund to County a proportionate refund of any pre-paid fees.

40.6 During the provision of Deliverables and/or services, Contractor may not disclaim any warranty, express or implied, and any such disclaimer shall be void.  Additionally, the warranties above shall not be deemed to exclude Contractor's standard warranties or other rights and warranties that the County may have or obtain.

40.7 Unless otherwise specified, the Contractor does not warrant that any Software provided hereunder is error-free or that it will run without immaterial interruption.

40.8 Contractor does not warrant and will have no responsibility for a claim to the extent that it arises directly from (A) a modification made by the County, unless such modification is approved or directed by Contractor, (B) use of Software in combination with or on products other than as specified by Contractor, or (C) misuse by the County.

40.9 Where Contractor resells Hardware or Software it purchased from a third party, and such third party offers additional or more advantageous warranties than those set forth herein, Contractor will pass through any such warranties to the County and will reasonably cooperate in enforcing them. Such warranty pass-through will be supplemental to, and not relieve Contractor from, Contractor's warranty obligations set forth above.

40.10 All warranties, including special warranties specified elsewhere herein, shall inure to theCounty, its successors, assigns, customer agencies, and governmental users of the Deliverables and/or services.

40.11 Should any Deliverable contain embedded or third party software without a license as specified in section 40.2.5, Contractor shall immediately obtain a license for County's benefit at no cost to the County. Said license shall conform to the requirements set forth in section 40.2.5.

## 41. COOPERATION WITH REVIEW

41.1 Contractor shall cooperate with County's periodic review of Contractor's performance. Contractor shall make itself available onsite to review the progress of the project and Agreement, as requested by the County, upon reasonable advanced notice.

41.2 Contractor agrees to extend to the County or his/her designees and/or designated auditor of the County, the right to monitor or otherwise evaluate all work performed and all records, including service records and procedures to assure that the project is achieving its purpose, that all applicable federal, state, and local laws and regulations are met, and that adequate internal fiscal controls are maintained.

## 42. AUDIT RIGHTS

42.1 Pursuant to California Government Code Section 8546.7, the parties acknowledge and agree that every contract involving the expenditure of public funds in excess of Ten Thousand Dollars ($10,000 USD) shall be subject to audit by the State Auditor.

42.2 All payments made under this Agreement shall be subject to an audit at County's option, and shall be adjusted in accordance with said audit. Adjustments that are found necessary as a result of auditing may be made from current billings.

42.3 Contractor shall be responsible for receiving, replying to, and complying with any audit exceptions set forth in any County audits. Contractor shall pay to County the full amount of any audit determined to be due as a result of County audit exceptions. This provision is in addition to other inspection and access rights specified in this Agreement.

## 43. ACCESS AND RETENTION OF RECORDS AND PROVISION OF REPORTS

43.1 Contractor shall maintain financial records adequate to show that County funds paid were used for purposes consistent with the terms of the Agreement between Contractor and County. Records shall be maintained during the terms of the Agreement and for a period of four (4) years from its termination, or until all claims have been resolved, whichever period is longer, unless a longer period is required under any contract.

43.2 All books, records, reports, and accounts maintained pursuant to the Agreement, or related to the Contractor's activities under the Agreement, shall be open to inspection, examination, and audit by County, federal and state regulatory agencies, and to parties whose Agreements with the County require such access. County shall have the right to obtain copies of any and all of the books and records maintained pursuant to the Agreement, upon the payment of reasonable charges for the copying of such records.

43.3 Contractor shall provide annual reports that include, at minimum, (i) the total contract release purchase order value for the County as a whole and individual County departments, (ii) the number of orders placed, the breakdown (by customer ID/department and County) of the quantity and dollar amount of each product and/or service ordered per year. Annual reports must be made available no later than thirty (30) calendar days of the Agreement anniversary date unless otherwise requested.

43.4 Contractor shall also provide quarterly reports to the County that show a breakdown by contract release purchase order (i) the order date (ii) ship date (iii) estimated arrival date (iv) actual arrival date (v) list of products, services and maintenance items (vi) the number and details of problem/service calls and department name that each such call pertains to (including unresolved problems). Quarterly reports must be made available to the County in electronic format, two (2) business days after the end of each quarter unless otherwise requested.

### 44. ACCESS TO BOOKS AND RECORDS PURSUANT TO THE SOCIAL SECURITY ACT

If and to the extent that, Section 1861 (v) (1) (1) of the Social Security Act (42 U.S.C. Section 1395x (v) (1) (1) is applicable, Contractor shall maintain such records and provide such information to County, to any payor which contracts with County and to applicable state and federal regulatory agencies, and shall permit such entities and agencies, at all reasonable times upon request, to access books, records and other papers relating to the Agreement hereunder, as may be required by applicable federal, state and local laws, regulations and ordinances. Contractor agrees to retain such books, records and information for a period of at least four (4) years from and after the termination of this Agreement. Furthermore, if Contractor carries out any of its duties hereunder, with a value or cost of Ten Thousand Dollars ($10,000 USD) or more over a twelve (12) month period, through a subcontract with a related organization, such subcontract shall contain these same requirements. This provision shall survive the termination of this Agreement regardless of the cause giving rise to the termination.

### 45. NON-DISCRIMINATION

Contractor shall comply with all applicable federal, state, and local laws and regulations, including Santa Clara County’s policies, concerning nondiscrimination and equal opportunity in contracting. Such laws include, but are not limited to, the following: Title VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act of 1990; The Rehabilitation Act of 1973 (§§ 503 and 504); California Fair Employment and Housing Act (Government Code §§ 12900 et seq.); and California Labor Code §§ 1101 and 1102. Contractor shall not discriminate against any employee, subcontractor or applicant for employment because of age, race, color, national origin, ancestry, religion, sex/gender, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status in the recruitment, selection for training including apprenticeship, hiring, employment, utilization, promotion, layoff, rates of pay or other forms of compensation. Nor shall Contractor discriminate in provision of services provided under this Agreement because of age, race, color, national origin, ancestry, religion, sex/gender, sexual orientation, mental disability, physical disability, medical condition, political beliefs, organizational affiliations, or marital status. Contractor's violation of this provision shall be deemed a material default by Contractor giving County a right to terminate the Agreement for cause.

## 46. DEBARMENT

Contractor represents and warrants that it, its employees, contractors, subcontractors or agents (collectively "Contractor") are not suspended, debarred, excluded, or ineligible for participation in Medicare, Medi-Cal or any other federal or state funded health care program, or from receiving federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration. Contractor must within thirty (30) calendar days advise the County if, during the term of this Agreement, Contractor becomes suspended, debarred, excluded or ineligible for participation in Medicare, Medi-Cal or any other federal or state funded health care program, as defined by 42. U.S.C. 1320a-7b(f), or from receiving federal funds as listed in the List of Parties Excluded from Federal Procurement or Non-procurement Programs issued by the Federal General Services Administration. Contractor shall defend, indemnify, and hold the County harmless for any loss or damage resulting from the conviction, debarment, exclusion or ineligibility of the Contractor.

## 47. RIGHTS IN WORK PRODUCT

47.1 All inventions, discoveries, intellectual property, technical communications and records originated or prepared by the Contractor pursuant to this Agreement including papers, reports, charts, computer programs, and other Documentation or improvements thereto, and including Contractor's administrative communications and records relating to this Agreement (collectively, the "Work Product"), shall be County's exclusive property. The provisions of this section may be revised in a SOW.

47.2 Software and other materials developed or otherwise obtained by or for Contractor or its affiliates independently of this Agreement or applicable purchase orders ("Pre-Existing Materials") do not constitute Work Product. If Contractor creates derivative works of Pre-Existing Materials, the elements of such derivative works created pursuant to this Contract constitute Work Product, but other elements do not. Nothing in this section will be construed to interfere with Contractor's or its affiliates' ownership of Pre-Existing Materials.

## 48. PROTECTION OF PROPRIETARY SOFTWARE AND OTHER PROPRIETARY DATA

48.1 The County agrees that all material appropriately marked or identified in writing as proprietary, and furnished hereunder are provided for County's exclusive use for the purposes of this Agreement only. All such proprietary data shall remain the property of the

Contractor. County agrees to take reasonable steps to insure that such proprietary data is not disclosed to others, without prior written consent of the Contractor, subject to the California Public Records Act ("CPRA").

48.2 The County will insure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed.

48.3 The County agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to licensed software and other proprietary data to satisfy its obligations under this Agreement with respect to use, copying, modification, protection and security of proprietary software and other proprietary data.

## 49. COUNTY DATA

49.1 "County Data" shall mean data and information received by Contractor from County. As between Contractor and County, all County Data shall remain the property of the County. Contractor shall not acquire any ownership interest in the County Data.

49.2 Contractor shall not, without County's written permission consent, use or disclose the County Data other than in the performance of its obligations under this Agreement.

49.3 Contractor shall be responsible for establishing and maintaining an information security program that is designed to ensure the security and confidentiality of County Data, protect against any anticipated threats or hazards to the security or integrity of County Data, protect against unauthorized access to or use of County Data that could result in substantial harm or inconvenience to County or any end users; and ensure the proper disposal of County data upon termination of this Agreement.

49.4 Contractor shall take appropriate action to address any incident of unauthorized access to County Data, including addressing and/or remedying the issue that resulted in such unauthorized access, notifying County as soon as possible of any incident of unauthorized access to County Data, or any other breach in Contractor's security that materially affects County or end users; and be responsible for ensuring compliance by its officers, employees, agents, and subcontractors with the confidentiality provisions hereof.

49.5 Should confidential and/or legally protected County Data be divulged to unauthorized third parties, Contractor shall comply with all applicable federal and state laws and regulations, including but not limited to California Civil Code Sections 1798.29 and 1798.82 at Contractor's sole expense (if applicable). Contractor shall not charge the County for any expenses associated with Contractor's compliance with the obligations set forth in this section.

## 50. SOFTWARE SOURCE CODE ESCROW

50.1 Software in Escrow: Contractor shall place in escrow with an independent escrow agent approved by the County, at Contractor's expense, all software that is relevant to functionality, setup, configuration, and operation of the System, including, but not limited to, a complete copy of the source and executable code, build scripts, object libraries, application program Interfaces, and complete Documentation of all aspects of the System including, but not limited to, compiling instructions, design Documentation, technical Documentation, user Documentation, hardware and software specifications, drawings, records, and related data (the "Deposit Material"). Contractor shall promptly deposit all new updates, versions or releases as they become available to customers. The Documentation shall include a sworn affidavit that the Deposit Material provided includes all relevant components mentioned in this section above and programs and materials necessary to compile and operate the System and use the source code for the purpose of maintaining the System as contemplated in Section 50.2 below. the reliability of the Equipment. Contractor shall add County as a beneficiary to its source code escrow agreement.

50.2 Access to Source Code: Pursuant to Appendix E, if Contractor ceases to do business (whether by bankruptcy, insolvency, or an assignment without consent of the County) or refuses to provide Maintenance (provided County is current on Maintenance fees), or if this Agreement is terminated for cause by County due to Contractor's material breach of this Agreement, Contractor shall make available to County the most recent Deposit Material. County shall have the right to copy, modify, and use said Deposit Material. Upon release of the Deposit Material, County agrees that (a) Contractor retains ownership of the Deposit Material, (b) the Deposit Material is licensed to County subject to the restrictions of this Agreement, (c) County may not remove or destroy any proprietary markings or legend placed upon or contained with the Deposit Material, (d) County may not market, sell, publish, disclose or otherwise make available the Deposit Material to any third party not permitted by this Agreement to use the Licensed Software, (e) County shall hold the Deposit Material of Contractor in strict confidence and not make any disclosure except as necessary for its use thereof, and (f) except when actually being utilized for the sole purpose of continuing the benefits afforded to County by the Agreement, County shall keep the Deposit Material in a restricted, limited access area with access thereto limited to designated personnel of County who have a need to use the Deposit Material for the purposes permitted hereunder for the duration of time as necessary to complete such permitted purpose. County shall return all Deposit Material if the event giving rise to the release of the Deposit Material is cured by Contractor.

50.3 Appendix E lists the annual fee to be paid by Contractor for third party escrow fees.

50.4 The source code may be made available by electronic transmission, at County's option.

## 51. CALIFORNIA PUBLIC RECORDS ACT INDEMNITY

The County is a public agency subject to the disclosure requirements of the CPRA. If the County receives a CPRA request for documents (as defined by the CPRA) and said request relates to the Deliverables and/or services provided pursuant to this Agreement, the County will notify Contractor of the request and confer with Contractor regarding an appropriate response to said request. If Contractor contends that any documents are Contractor's confidential or proprietary material, not subject to the CPRA, and/or exempt from the CPRA, and Contractor wishes to prevent disclosure of said documents, Contractor shall instruct County to withhold said documents. If Contractor fails to respond to County in writing prior to the County's deadline for responding to the CPRA request, the County may disclose the requested information under the CPRA without liability to the County. Contractor shall defend, indemnify and hold the County harmless against any claim, action or litigation (including but not limited to all judgments, costs, fees, and reasonable attorneys fees) that may result from denial of a CPRA request.

### 52. SEVERABILITY

Should any part of the Agreement between County and the Contractor or any individual contract release purchase order be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect the validity of the remainder of the Agreement or any individual contract release purchase order which shall continue in full force and effect, provided that such remainder can, absent the excised portion, be reasonably interpreted to give the effect to the intentions of the parties.

### 53. NON-WAIVER

No waiver of a breach, failure of any condition, or any right or remedy contained in or granted by the provisions of this Agreement will be effective unless it is in writing and signed by County. No waiver of any breach, failure, right, or remedy will be deemed a waiver of any other breach, failure, right, or remedy, whether or not similar, nor will any waiver constitute a continuing waiver unless the writing signed by the County so specifies.

### 54. USE OF COUNTY'S NAME FOR COMMERCIAL PURPOSES

Contractor may not use the name of the County or reference any endorsement from the County in any fashion for any purpose, without the prior express written consent of the County as provided by the Director of Procurement, or authorized designee.

### 55. HEADINGS AND TITLES

The titles and headings in this Agreement are included principally for convenience and do not by themselves affect the construction or interpretation of any provision in this Agreement, nor affect any of the rights or obligations of the parties to this Agreement.

### 56. HANDWRITTEN OR TYPED WORDS

Handwritten or typed words have no greater weight than printed words in the interpretation or construction of this Agreement.

### 57. AMBIGUITIES

Any rule of construction to the effect that ambiguities are to be resolved against the drafting party does not apply in interpreting this Agreement. Should any ambiguities or conflicts between contract terms and conditions contained in this Agreement and its Appendices exist, the terms and conditions in this Agreement shall control over its appendices.

### 58. ENTIRE AGREEMENT

This Agreement and its appendices (if any) constitute the final, complete and exclusive statement of the terms of the agreement between the parties. It incorporates and supersedes all the agreements, covenants and understandings between the parties concerning the subject matter hereof, and all such agreements, covenants and understandings have been merged into this Agreement. No prior or contemporaneous agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

**59. EXECUTION & COUNTERPARTS**

This Agreement may be executed in one or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. The parties agree that this Agreement, its amendments, and ancillary agreements to be entered into in connection with this Agreement will be considered signed when the signature of a party is delivered by facsimile transmission. Such facsimile signature must be treated in all respects as having the same effect as an original signature. The original signature copy must be sent to the County by United States Postal Service mail, sent by courier or delivered by hand.

**60. NOTICES**

All deliveries, notices, requests, demands or other communications provided for or required by this Agreement shall be in writing and shall be deemed to have been given when sent by registered or certified mail, return receipt requested; when sent by overnight carrier; or upon email confirmation to sender of receipt of a facsimile communication which is followed by a mailed hard copy from sender. Notices shall be addressed to:

**COUNTY:**
Name:______________________________
Contract Administrator
c/o Procurement Department
2310 North First Street, Suite 201
San Jose, CA 95131-1040

**CONTRACTOR:**

Name:______________________________

Title:______________________________

Company:______________________________

Address 1:______________________________

Address 2:______________________________

City:______________________________

State:______________________________

Zip:________________________________

Each party may designate a different person and address by sending written notice to the other party, to be effective no sooner than ten (10) calendar days after the date of the notice.

### 61. ACCOUNT MANAGER

Contractor must assign an Account Manager to the County to facilitate the contractual relationship, be fully responsible and accountable for fulfilling the County's requirements. Contractor represents and warrants that such person will ensure that the County receives adequate pre- and post-sales support, problem resolution assistance and required information on a timely basis.

### 62. SURVIVAL

All representations, warranties, indemnities, and covenants contained in this Agreement, or in any instrument, certificate, appendix, or other writing intended by the parties to be a part of their Agreement, will survive the termination of this Agreement.

### 63. GOVERNING LAW, JURISDICTION AND VENUE

This Agreement shall be construed and interpreted according to the laws of the State of California, excluding its conflict of law principles. Proper venue for legal actions shall be exclusively vested in state court in the County of Santa Clara. The parties agree that subject matter and personal jurisdiction are proper in state court in the County of Santa Clara, and waive all venue objections.

### 64. HIPAA

Contractor shall comply with Appendix ___, which sets forth certain requirements pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

### 65. NO SMOKING

Contractor and its employees, agents and subcontractors, shall comply with the County's No-Smoking Policy, as set forth in the Board of Supervisors Policy Manual section 3.47 (as amended from time to time), which prohibits smoking: (1) at the Santa Clara Valley Medical Center Campus and all County-owned and operated health facilities, (2) within 30 feet surrounding County-owned buildings and leased buildings where the County is the sole occupant, and (3) in all County vehicles.

### 66. REMOTE ACCESS AND USER RESPONSIBILITY

Appendix ___ of this Agreement lists the remote access and user responsibility requirements, terms and conditions. Contractor shall comply with this Appendix.

### 67. BEVERAGE NUTRITIONAL CRITERIA

If Contractor provides beverages through County departments, or at County programs, sponsored meetings, sponsored events, or at County owned/operated facilities, Contractor shall not use County funds to purchase beverages that do not meet the County's nutritional beverage criteria, if applicable. The six categories of nutritional beverages that meet these criteria are (1) water with no additives; (2) 100% fruit juices with no added sugars, artificial flavors or colors (limited to a maximum of 10 ounces per container); (3) dairy milk, non-fat, 1% and 2% only, no flavored milks; (4) plant derived (i.e., rice, almond, soy, etc.) milks (no flavored milks); (5) artificially-sweetened, calorie-reduced beverages that do not exceed 50 calories per 12-ounce container (teas, electrolyte replacements); and (6) other non-caloric beverages, such as coffee, tea, and diet sodas. These criteria may be waived in the event of an emergency or in light of medical necessity.

## 68. ASSIGNMENT OF CLAYTON ACT, CARTWRIGHT ACT CLAIMS

Contractor hereby assigns to the County all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the Contractor for sale to the County pursuant to this agreement.

## 69. ELECTRONIC COPY OF SIGNED AGREEMENT

All parties agree that an electronic copy of a signed contract shall have the same force and effect as an original signed contract provided that the Contractor agrees to deliver to the County the original signed contract within 7 business days of sending an electronic copy. The term "electronic copy" for purposes of this provision refers to a transmission by facsimile or electronic mail in a portable document format.

# ATTACHMENT 2

## EXHIBIT B3 Revised 4/2002
## INSURANCE REQUIREMENTS

### Indemnity

The Contractor shall indemnify, defend, and hold harmless the County of Santa Clara (hereinafter "County"), its officers, agents and employees from any claim, liability, loss, injury or damage arising out of, or in connection with, performance of this Agreement by Contractor and/or its agents, employees or sub-contractors, excepting only loss, injury or damage caused by the sole negligence or willful misconduct of personnel employed by the County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for the County. The Contractor shall reimburse the County for all costs, attorneys' fees, expenses and liabilities incurred with respect to any litigation in which the Contractor is obligated to indemnify, defend and hold harmless the County under this Agreement.

### Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. Evidence of Coverage

Prior to commencement of this Agreement, the Contractor shall provide a Certificate of Insurance certifying that coverage as required herein has been obtained. Individual endorsements executed by the insurance carrier shall accompany the certificate. In addition, a certified copy of the policy or policies shall be provided by the Contractor upon request.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. Qualifying Insurers

All coverages, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation

All coverage as required herein shall not be canceled or changed so as to no longer meet the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

| | | |
|---|---|---|
| a. Each occurrence | - | $1,000,000 |
| b. General aggregate | - | $2,000,000 |
| c. Personal Injury | - | $1,000,000 |

2. General liability coverage shall include:

   a. Premises and Operations
   b. Personal Injury liability
   c. Severability of interest

3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

   **Additional Insured Endorsement,** which shall read:

   > "County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds."

   Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance
   For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to owned, non-owned and hired vehicles.

4a. Aircraft/Watercraft Liability Insurance (Required if Contractor or any of its agents or subcontractors will operate aircraft or watercraft in the scope of the Agreement)

   For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to all owned non-owned and hired aircraft/watercraft.

5. Workers' Compensation and Employer's Liability Insurance
   a. Statutory California Workers' Compensation coverage including broad form all-states coverage.
   b. Employer's Liability coverage for not less than one million dollars ($1,000,000) per occurrence.

6. Professional Errors and Omissions Liability Insurance
   a. Coverage shall be in an amount of not less than one million dollars ($1,000,000) per occurrence/aggregate.
   b. If coverage contains a deductible or self-retention, it shall not be greater than fifty thousand dollars ($50,000) per occurrence/event.
   c. Coverage as required herein shall be maintained for a minimum of two years following termination or completion of this Agreement.

7. Claims Made Coverage
   If coverage is written on a claims made basis, the Certificate of Insurance shall clearly state so. In addition to coverage requirements above, such policy shall provide that:

   a. Policy retroactive date coincides with or precedes the Consultant's start of work (including subsequent policies purchased as renewals or replacements).
   b. Policy allows for reporting of circumstances or incidents that might give rise to future claims.

E. Special Provisions

The following provisions shall apply to this Agreement:

1. The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning indemnification.

2. The County acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractors obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.

3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned coverages, or Contractor may insure subcontractors under its own policies.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

# ATTACHMENT 3

## BUSINESS ASSOCIATE AGREEMENT (HIPAA AND HITECH)

WHEREAS, County of Santa Clara ("County" or "Covered Entity") is a Covered Entity, as defined below, and wishes to disclose certain Protected Health Information ("PHI") to [Enter Name of Contractor_____] "Business Associate" pursuant to the terms of the Agreement and this Business Associate Agreement ("BAA"); and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable law; and

WHEREAS, as part of the HIPAA Regulations, the Privacy Rule and the Security Rule (defined below) require Covered Entity to enter into a contract containing specific requirements with Business Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this BAA.

In consideration of the mutual promises below and the exchange of information pursuant to the BAA, the parties agree as follows:

### I. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in the BAA have the same meaning as defined under the Health Insurance Portability and Accountability Act of 1996, 42 USC §§ 1320d et seq. ("HIPAA") and the implementing regulations and with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws.

**Privacy Breach** Any acquisition, access, use or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

**Business Associate is** a person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

**Covered Entity** shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. Section 160.103.

**Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

**Electronic Protected Health Information** means Protected Health Information that is maintained in or transmitted by electronic media.

**Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

**Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.501.

**Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

**Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.103. Protected Health Information includes Electronic Protected Health Information [45 C.F.R. Sections 160.103].

**Protected Information** shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on Covered Entity's behalf.

**Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

**Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

## II. Duties & Responsibilities of Business Associate

**a. Permitted Uses.** Business Associate shall not use Protected Information except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and the BAA. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used by Covered Entity. However, Business Associate may use Protected Information (i) for the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) for Data Aggregation purposes for the Health Care Operations of Covered Entity [45 C.F.R. Sections 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)].

b. **Permitted Disclosures.** Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Agreement and as permitted under the Agreement and the BAA. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so disclosed by Covered Entity. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; (iii) as required by law; or (iv) for Data Aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any breaches of confidentiality of the Protected Information within 10 calendar days of discovery, to the extent it has obtained knowledge of such breach [42 U.S.C. Section 17932; 45 C.F.R. Sections 164.504(e)(2)(i), 164.504(e)(2)(i)(B), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(ii)].

c. **Prohibited Uses and Disclosures.** Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the PHI solely relates [42 U.S.C. Section 17935(a)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act, 42 U.S.C. section 17935(d)(2); however, this prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Agreement.

d. **Appropriate Safeguards.** Business Associate shall implement appropriate administrative, technological and physical safeguards as are necessary to prevent the use or disclosure of Protected Information otherwise than as permitted by the Agreement and the BAA that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Information, in accordance with 45 C.F.R. Sections 164.308, 164.310, 164.312 and 164.316. [45 C.F.R. Section 164.504(e) (2) (ii) (B); 45 C.F.R. Section 164.308(b)]. Business Associate shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. Section 164.316 [42 U.S.C. Section 17931].

e. **Reporting of Improper Access, Use or Disclosure.** Business Associate shall report to Covered Entity in writing any access, use or disclosure of Protected Information not permitted by the Agreement and BAA, and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than 10 calendar days after discovery [42 U.S.C. Section 17921; 45 C.F.R. Section 164.504(e) (2) (ii) (C); 45 C.F.R. Section 164.308(b)]. All reports to Covered Entity pursuant to this section shall be sent to the Covered Entity Compliance Officer by facsimile and U.S. mail using the following contact information:

Compliance & Privacy Officer
Santa Clara Valley Health & Hospital System
2325 Enborg Lane, Suite 360
San Jose, CA 95128
Facsimile (408) 885-6886
Telephone (408) 885-3794

The breach notice must contain: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known, (2) the location of the breached information; (3) a description of the types of PHI that were involved in the breach,(4) Safeguards in place prior to the breach; (5) Actions taken in response to the breach; (3) any steps individuals should take to protect themselves from potential harm resulting from the breach, (4) a brief description of what the business associate is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches, and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address. [45 C.F.R Section 164.410] Business Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

f. **Business Associate's Agents.** Business Associate shall ensure that any agents, including subcontractors, to whom it provides Protected Information, agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such PHI and implement the safeguards required by paragraph c above with respect to Electronic PHI [45 C.F.R. Section 164.504(e) (2) (ii) (D); 45 C.F.R. Section 164.308(b)]. Business Associate shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation (see 45 C.F.R. Sections 164.530(f) and 164.530(e) (1)).

g. **Access to Protected Information.** Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524 [45 CF.R. Section 164.504(e) (2) (ii) (E)]. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e).

h. **Electronic PHI.** If Business Associate receives, creates, transmits or maintains EPHI on behalf of Covered Entity, Business Associate will, in addition, do the following:

(1) Develop, implement, maintain and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of

CFR to preserve the integrity and confidentiality of all electronically maintained or transmitted PHI received from or on behalf of Covered Entity.

(2) Document and keep these security measures current and available for inspection by Covered Entity.

(3) Ensure that any agent, including a subcontractor, to whom the Business Associate provides EPHI, agrees to implement reasonable and appropriate safeguards to protect it.

(4) Report to the Covered Entity any Security Incident of which it becomes aware. For the purposes of this BAA and the Agreement, Security Incident means, as set forth in 45 C.F.R section 164.304, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

i. **Amendment of PHI.** Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to the County for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule. If any individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

j. **Accounting Rights.** Promptly upon any disclosure of Protected Information for which Covered Entity is required to account to an individual, Business Associate and its agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, and the HITECH Act, as determined by Covered Entity. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an electronic health record and is subject to this requirement.

At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall within five (5) days of a request forward it to Covered Entity in writing. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in the Agreement, including this BAA.

**k. Governmental Access to Records.** Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining Business Associate s compliance with the Privacy Rule. Business Associate shall provide to Covered Entity a copy of any Protected Information that Business Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary.

**l. Minimum Necessary.** Business Associate (and its agents or subcontractors) shall request, use and disclose only the minimum amount of Protected Information necessary to accomplish the purpose of the request, use, or disclosure. Business Associate understands and agrees that the definition of "minimum necessary" is in flux and shall keep itself informed of guidance issued by the Secretary with respect to what constitutes "minimum necessary."

**m. Data Ownership.** Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information.

**n. Audits, Inspection and Enforcement.** Within ten (10) days of a written request by Covered Entity, Business Associate and its agents or subcontractors shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this BAA for the purpose of determining whether Business Associate has complied with this BAA; provided, however, that (i) Business Associate and Covered Entity shall mutually agree in advance upon the scope, timing and location of such an inspection, (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate .

The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate 's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with the BAA, nor does Covered Entity's (i) failure to detect or (ii) detection, but failure to notify Business Associate or require Business Associate 's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the Agreement or BAA, Business Associate shall notify Covered Entity within ten (10) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights.

## III. Termination

**a. Material Breach**. A breach by Business Associate of any provision of this BAA, as determined by Covered Entity, shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement, any provision in the Agreement to the contrary notwithstanding [45 C.F.R. Section 164.504(e)(2)(iii)].

**b. Judicial or Administrative Proceedings.** Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate has been joined.

**c. Effect of Termination.** Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, as determined by Covered Entity, Business Associate shall continue to extend the protections of Section 2 of the BAA to such information, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. [45 C.F.R. Section 164.504(e) (ii) (2(I)]. If Covered Entity elects destruction of the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

## IV. General Provisions

**a. Indemnification.** In addition to the indemnification language in the Agreement, Business Associate agrees to be responsible for, and defend, indemnify and hold harmless the County for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines and assessments that may be made against SCVHHS or the Business Associate for any privacy breaches or late reporting.

**b. Disclaimer.** The County makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

**c. Amendment to Comply with Law.** The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Agreement and/or BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that the County must receive satisfactory written assurance from Business Associate that Business Associate will adequately safeguard all Protected Information.

Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to the BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule or other applicable laws. The County may terminate the Agreement upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend the Agreement or BAA when requested by the County pursuant to this Section or (ii)

Business Associate does not enter not enter into an amendment to the Agreement or BAA providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

**d. Assistance in Litigation of Administrative Proceedings.** Business Associate shall make itself, and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement or BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its directors, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee or agent is named adverse party.

**e. No Third-Party Beneficiaries.** Nothing express or implied in the Agreement or BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

**f. Effect on Agreement.** Except as specifically required to implement the purposes of the BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

**g. Interpretation.** The provisions of this BAA shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this BAA. The BAA and the Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule and the Security Rule.

**h. Survivorship.** The respective rights and responsibilities of Business Associate related to the handling of PHI survive termination of this Agreement.

# ATTACHMENT 4

## USER RESPONSIBILITY AND VENDOR REMOTE ACCESS STATEMENTS

### *INFORMATION TECHNOLOGY*
### *USER RESPONSIBILITY STATEMENT AND INSTRUCTIONS*

In May 1995 the Board of Supervisors charged each County organization with the responsibility for ensuring that all individuals within the organization had read and signed a statement of responsibility concerning use of the County's networks and information systems. This Statement is intended as a <u>minimum</u> Statement of User Responsibility, and individual County Agencies and Departments may make additions to strengthen it as necessary to meet any special requirements within their own environments.

- The User Responsibility Statement must be signed by everyone who might reasonably require access to a County network and/or information system, which includes County employees, consultants, contractors, sub-contractors, vendors, volunteers and any other authorized individual who is permitted access. All Users who are allowed to access County resources remotely must also sign an additional attachment specifically related to remote access; this is provided as Attachment 3.
- Each County organization should identify a "User Responsibility Statement Administrator." This is an occasional personnel function that should NOT be filled by a member of the organization's Information System's support staff. A good choice would be a personnel administrator or office staff responsible for other routine personnel issues. The User Responsibility Statement Administrator is responsible for the following tasks:

1. Identifying those employees, contractors and others within the organization that will need to read and sign the Statement.
2. Managing the signing process, including arranging for any briefings that are held in conjunction with users signing the Statement.
3. Maintaining the signed Statements.
4. Documenting in the Agency / Departmental IT Security Plan that the Statements have been signed by all appropriate employees, contractors, and others.
5. Ensuring that new employees, contractors, etc. read and sign the Statement.

- County organizations must identify all individuals who need to sign the Statement. For most organizations, the easiest approach would be to have everyone read and sign a Statement, but in some unusual cases it might make sense to exclude specific workgroups who clearly will never have the need to access a County computer or network.
- Following identification of the appropriate User communities, the Statements should be distributed for reading and signing. One possible method for accomplishing this is an all-staff briefing session, during which staff, contractors, etc. are presented with an overview of the Statement and then asked to sign it.
- It should be noted that individuals who sign the Statement are not required to agree with all of the Statement's provisions but that by signing they are acknowledging that they have read the Statement and understood its contents. The signer also acknowledges that violation of any of the Statement's provisions may result in disciplinary action and/or criminal prosecution.
- In rare situations where an individual refuses to sign the Statement the responsible Agency / Department may choose to read the Statement to the involved individual who will be required to verbally acknowledge understanding with two or more responsible managers present who will attest in writing that the reading and verbal attestation of understanding occurred. Failing a verbal acknowledgement of understanding the involved individual shall be denied access to all County information systems and networks.
- Each County organization is responsible for storing and maintaining all of the signed Statements. It is required that all County organizations have their users re-execute the Statement whenever there is an update or other change to the Statement. The Department Heads will be notified by the CIO's office of any updates or other changes to the Statement. It is recommended that all County organizations have their users re-execute the Statement annually. Also, all users that have remote access capabilities into the County must read and sign Attachment 3 of the Statement.

# INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT

This User Responsibility Statement establishes a uniform, County-wide set of minimum responsibilities associated with being granted access to County information systems and/or County networks.

## Definitions

*County information systems and networks* include all County-owned, rented, or leased desktop computers, laptop computers, handheld devices (including smart phones, wireless PDA's and Pocket PC's), equipment, networks, application systems, data bases and software; these items are typically under the direct control and management of County information system staff. Also included are information systems and networks under control and management of a service provider for use by the County.

*Users* includes full-time and part-time employees who are on the permanent County payroll, as well as other authorized individuals such as contractors, sub-contractors, consultants, temporary personnel, unpaid volunteers and any other authorized individual permitted access to County information systems and/or networks.

*County-owned information/data* is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under control and management of a service provider for use by the County. This information/data is the exclusive property of the County of Santa Clara, unless excepted through constitutional provision, State or Federal statute, case law, or contract.

A *public record* is any writing, including electronic documents, relating to the conduct of the people's business.

## 1. General Code of Responsibility

The following General Code of Responsibility defines the basic standards for user interaction with County information systems and networks. All Users of County information systems and networks are required to comply with these standards.

1.1 Users are personally responsible for knowing and understanding the appropriate standards for User conduct, and are personally responsible for any actions they take that do not comply with County policies and standards.

1.2 Users must comply with County standards for password definition, use, and management. If a User is unclear as to the appropriate standards, it is the responsibility of the User to ask for guidance from their information systems support staff or Agency / Department management.

1.3 Users may not install, configure, or use any modem, any connection to a non-County network or system, or any wireless device, on any County system or network unless authorized to do so in writing by their designated departmental information systems support staff. If authorized to install, configure or use such a device or capability, Users must comply with all additional, applicable County standards designed to ensure the privacy and protection of data.

1.4 All connections between County information systems/networks and non-County systems/networks, including the Internet, must be approved by the County Chief Information Officer (CIO), or designee, and by the head of the involved Agency/Department. Users, including members of the County's information system support staff, are prohibited from implementing such connections without obtaining this approval in writing.

1.5 No personally owned desktop computer, laptop computer, handheld and/or wireless device, or any other device may be attached to a County network unless such attachment is authorized in writing by designated departmental information systems support staff.

1.6 Users must not attempt to circumvent legal guidelines on software use and licensing by copying software. If a User is unclear as to whether a piece of software may be legitimately copied, it is the responsibility of the User to check with designated departmental information systems support staff.

1.7 Users may not install software on any County system unless specifically authorized to do so in writing by designated departmental information systems support staff.

1.8 Users are asked to be aware of security issues, and are encouraged to report incidents of security breaches (e.g., installation of an unauthorized device) to designated information systems support staff.

1.9 Users must understand and respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

- Users must not attempt to access County systems or information unless authorized to do so and there is a legitimate business need for such access.
- Users must not disclose information to anyone who does not have a legitimate need for that information.
- Users must not make or store printed or media-based (e.g., CD or floppy disk) copies of information unless it is a necessary part of that user's job.

1.10 Users must understand and respect the importance of County-owned data as a valuable asset. In particular:

- Users must not change or delete data or information unless performing such changes or deletions is a legitimate part of the user's job function.
- Users must avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

1.11 Users should be aware that electronic information transported across any County network, or residing in any County information system, is potentially subject to access by technical support staff, other County Users, and the general public. There are within the County IT environment systems and networks that have been made secure and private but in the absence of such special measures Users should not presume any level of data privacy for information transmitted over a County network, or stored within a County information system.

1.12 In general, Users must not use County systems or networks for personal activities that cannot be shown to either facilitate work tasks or increase job productivity. However, reasonable incidental (deminimus) personal use of County IT resources, such as Internet access and email, is allowed as long as such use does not interfere with the performance of work duties or the operation of the County's information systems. If a User is unclear as to appropriate personal uses, it is the responsibility of the User to ask for guidance from their Agency / Department management.

1.13 All information resources on any County information system or network are the property of the County and are therefore subject to County policies regarding acceptable use. No employee or other authorized User may use any County owned network, computer system, handheld and/or wireless device, cell phone or any other device or data for the following purposes:

- Personal profit, including commercial solicitation or conducting or pursuing their own business interested or those of another organization.
- Unlawful or illegal activities, including the downloading of licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.
- To access, create, transmit, print, download or solicit material that is or may be construed to be harassing or demeaning toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.
- To access, create, transmit, print, download or solicit sexually-oriented messages or images.
- The knowing propagation or downloading of viruses or other contaminants.
- The dissemination of hoaxes, chain letters, or advertisements.

1.14 Users that are employed by, or otherwise belong to, a HIPAA impacted Agency / Department are responsible for understanding and carrying out their responsibilities and duties as identified in the County HIPAA policies and procedures training.

1.15 Users should refer to the County's email retention policy for guidance with respect to the retention of email messages.

1.16 Users may not configure, access, use, or participate in those Internet services that have been prohibited by County policy, including but not limited to Internet Instant Messaging services (such as AOL Instant Messaging), Internet email services (such as Hotmail), and peer-to-peer networking services (such as Kazaa), unless specifically authorized to do so in writing. All use of such services, even at a Departmental level, is subject to written approval and authorization procedures by the Department Head and the County CIO.

1.17 Users shall not use an internal County email account assigned to another individual to either send or receive emails.

1.18 Users shall not configure their email account to automatically forward email messages to an Internet or other external email system unless specifically authorized to do so in writing by their Department Head and the County CIO. Email messages that are manually forwarded must not contain information that is classified as confidential or restricted.

## Acknowledgement of Receipt

This statement hereby incorporates Attachment 1 - Board of Supervisors Approved policy on "E-Mail", Attachment 2 – Board of Supervisors Approved Policy on "Internet Usage" and Attachment 3 - Additional Responsibilities for Users Accessing County IT Assets from Non-County (Remote) Locations. Attachment C only applies to individuals that have been granted remote access privileges and should only be signed by those specific individuals. By signing this Statement, the following individual signifies that the County's User Responsibility Statement has been read and its contents understood. The signer also acknowledges that violation of any of its provisions may result in disciplinary action, leading up to and including termination and/or criminal prosecution.

The signor also acknowledges that this Statement will still be in effect following any transfer to another County Agency or Department, and that all of its provisions will continue to apply to the undersigned.

User Signature ____________________________________________

Print User Name ____________________________________________

Agency/Department ____________________________________________

Date Signed ____________________________________________

## ATTACHMENT 4.1 - BOARD OF SUPERVISOR'S APPROVED POLICY ON "E-MAIL"

### Purpose of Policy

This policy addresses access to and the disclosure of information created, transmitted, received and stored via the County's e-mail systems. Access to e-mail is provided to employees and occasionally to other persons such as authorized contractors or volunteers (collectively referred to as "employees" in this policy), to assist them to perform their work, and their use of email must not jeopardize operation of the County's information systems or the reputation and integrity of the County. This policy is intended to ensure that County employees know their rights and responsibilities in using e-mail, and to ensure the appropriate, cost effective, and efficient use of County e-mail systems.

Use of the County's information systems must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et. seq. requires the County to make all public records available for inspection and to provide copies upon request. A public record is any writing, including electronic documents, relating to the conduct of the people's business. Any information sent via e-mail may be subject to disclosure under the CPRA or requested in the process of litigation discovery. In addition, no use of licensed or copyrighted material should be made without permission from the holder of the license or copyright.

### Appropriate Use of E-Mail

E-mail is provided as a business tool, however, its reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with performance of work duties nor with the operation of the County's information systems.

A. No employee may use e-mail for inappropriate purposes, such as, but not limited to the following:

(1) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization.

(2) Unlawful or illegal activities.

(3) Creation or dissemination of harassing or demeaning statements toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.

(4) The dissemination of hoaxes, chain letters, or advertisements.

(5) The knowing propagation or downloading of viruses or other contaminants.

B. Employees should not create, send, forward, or reply to distribution lists concerning non-County business. Employees should consider the impact on the County's networks when creating and using large, work-related distribution lists.

## Access to Messages

A. Employees should have no expectation of privacy in any messages sent via e-mail over the County's networks; employees should not use the system for any messages that they wish to remain private. Any electronic information transported across the County's networks is potentially subject to access by technical support staff, and review, monitoring, and disclosure by an audit authority designated by an employee's department head (or by the County Executive with respect to usage by department and agency heads). All computer applications, programs, and work-related information created or stored by employees on the County's information systems are County property. If employees make incidental use of the e-mail system to transmit personal messages, such messages will be treated no differently from other messages.

B. The use of employee passwords and other message protection measures, other than those specifically authorized by the County, are prohibited. The County's authorization to use a password or other data protection measure shall not constitute consent by the County to maintain the messages as private.

C. This policy does not supplant the legal protections available to shield confidential, internal County communications from third party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to state law mandating confidentiality for specific subject matter.

## Retention Policy

E-mail that is not necessary to the ordinary course of business should be routinely deleted.

## Enforcement

Any violation of the County's e-mail policy may result in appropriate disciplinary action up to and including termination. Any improper e-mail will not be disclosed by the County to others except to the extent necessary to consider and to implement discipline, for other employment related purposes, or to respond to litigation requests. Potential criminal conduct which is revealed by improper e-mail will be referred to the appropriate law enforcement authorities.

## ATTACHMENT 4.2 – BOARD OF SUPERVISOR'S APPROVED POLICY ON "INTERNET USAGE"

### Purpose of Policy

The Internet has become an increasingly important source of information for County employees. Many County employees, and occasionally others such as contractors and volunteers (collectively referred to in this policy as "employees"), are provided access to the Internet to assist in the performance of their work for the County. However, the diversity of information available on the Internet brings with it the potential for abuse. This policy is intended to ensure that County employees know their rights and responsibilities in using the Internet, and to ensure the appropriate, cost effective, and efficient use of County Internet access capabilities.

Use of the Internet via the County's system must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et. seq. requires the County to make all public records available for inspection and to provide copies upon request. A public record is any writing, including electronic documents, relating to the conduct of the people's business. The CPRA applies to information processed, sent and stored on the Internet. Additionally, records of Internet use may be requested during litigation discovery. No use of licensed or copyrighted material should be made without permission from the holder of the license or copyright.

### Appropriate Internet Use

Access to the Internet is provided as a business tool, however, its reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with performance of work duties or the operation of County information systems.

A. No employee, however, may use the Internet for inappropriate purposes, such as, but not limited to the following:

(1) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization.

(2) Unlawful or illegal activities, including the downloading of licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.

(3) To access, create, transmit, print, download or solicit material that is or may be construed to be harassing or demeaning toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation.

(4) To access, create, transmit, print, download or solicit sexually-oriented messages or images.

(5) The knowing propagation or downloading of viruses or other contaminants.

B. Internet Relay Chat channels or other Internet forums such as newsgroups or net servers may be used only to conduct work-related business.

## Access to Usage Records

A. Employees should have no expectation of privacy in their usage of the Internet. An audit authority designated by a department head may monitor usage of the Internet by department employees, including reviewing a list of sites accessed by an employee within the department; audit and examination of usage by an agency or department head shall be performed by a person designated by the County Executive. For this purpose, records of access to sites, materials and services on the Internet may be recorded and retained for a time period set by the County. The County or department head may restrict access to certain sites that it deems are not necessary for business purposes.

B. This policy does not supplant the legal protections available to shield confidential, internal County communications from third party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to state law mandating confidentiality for specific subject matter.

## Enforcement

Violation of the County’s policy on Internet use may result in appropriate disciplinary action up to and including termination. Any improper Internet usage will not be disclosed by the County to others except to the extent necessary to consider and to implement discipline, for other employment related purposes, or to respond to litigation requests. Potential criminal conduct which is revealed by inappropriate Internet usage will be referred to the appropriate law enforcement authorities.

## Attachment 3 – Additional Responsibilities for Users Accessing County IT Assets from Non-County (Remote) Locations

"*Remote access*" involves access to County Information Technology (IT) assets from a non-County infrastructure, no matter what technology is used to accomplish such access. This includes (but is not limited to) access to County IT assets from employee homes using modem-based or Internet connectivity, such as DSL or cable modem access. Systems that might be employed to accomplish such access include, but are not limited to, personal computers, workstations, laptops, palm-tops, "smart" phones, and any device that has network capabilities, such as routers and switches.

All remote access to County IT assets must be via secure, centralized, County-controlled mechanisms and technologies that have been reviewed and approved by the County CIO or designee. Users are not permitted to implement, configure, or use any remote access mechanism other than those that have been formally reviewed and approved in this manner. These approved technologies must include the following security features:

- Two-Factor Authentication: A strong method of authentication that verifies that the User is in fact the individual he is claiming to be. The two-factor authentication approach requires that the User provide two of the following three items: 1) something that the user has (such as a token card access device), 2) something that the user knows (such as a password or Personal Identification Number (PIN)), and 3) something that the user "is" (such as a fingerprint or retina scan). An equal or stronger authentication method may be used if approved by the County CIO or designee.
- User-specific, centrally controlled authorization (permissions) that limit User privileges once the User has been authenticated.
- Audit tools that create detailed records of all remote access attempts and remote access sessions including user identifier, date and time of access attempt.

The following regulations, responsibilities, and limitations apply to all Users attempting remote access to County IT assets, where a "User" is defined as "*any individual accessing and/or using County IT assets, including employees, contractors, sub-contractor, consultants, part-time employees, volunteers, and any other authorized individual attempting access or use of the County's IT infrastructure*."

- Remote access is supported and provided only for those Users that have both read and signed the County's general User Responsibility Statement.
- Approval for use of County remote access mechanisms will be granted to a specific User, by the appropriate Agency/Department Head or designee, only on an individual, case-by-case basis. In general, approval for remote access is given only to those Users that require such access in order to perform their job functions.

- Remote access sessions may be monitored, recorded, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when accessing County IT networks, systems, or data.
- Remote devices used for accessing County networks or systems may never be simultaneously connected to a non-County network or system, either directly or indirectly, while being used for remote access to the County, unless such a network or system is part of a remote access infrastructure approved by the County CIO or designee.
- All devices used to remotely access County IT assets must be configured according to County-approved security standards. These include installed, active, and current anti-virus software; software or hardware-based firewall; and any other security software or security-related system configurations that have been required and approved by the County.
- Users that have been provided with County-owned devices intended for remote access use, such as laptops and other portable devices will take all reasonable care to ensure that these devices are protected from damage, access by third parties, loss, or theft.
- Remote access Users will practice due diligence in protecting the integrity of County networks, systems, and data while remotely accessing County IT assets. Specifically, all remote access sessions are subject to all other relevant County IT security policies and standards, including Local User Authentication, Data Classification, Internet Use, and Email.

**Signature of Receipt:**

By signing this statement, the User signifies that the contents of this Statement have been reviewed and understood, and that violation of its provisions may result in disciplinary action, leading up to and including termination and/or criminal prosecution.

The signer also acknowledges that this Statement will still be in effect following any transfer to another County Agency or Department, and that all of its provisions will continue to apply to the undersigned.

Agency: ____________________________

Signature: ____________________________ Date Signed: _________

## *VENDOR REMOTE ACCESS*

### 1. Scope of Access

a. "Remote Access" is the act of accessing County of Santa Clara ("County") systems from a non-County network infrastructure. "Systems" include personal computers, workstations, servers, mainframes, phone systems, and/or any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices).

b. County hereby grants Remote Access privileges for Contractor to access the following County systems, at the locations listed, collectively referred to as "IS," in accordance with the terms of the Agreement:

County Systems: ____________

c. All other forms of access to the named Systems, or to any County System that is not specifically named, is prohibited.

d. Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in the Agreement including, but not limited to, supporting Contractor-installed programs. Any access to IS and/or County data or information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any penalty allowed by law.

e. County will review the scope of Contractor's Remote Access rights periodically. In no instance will Contractor's Remote Access rights be reduced, limited or modified in a way that prevents or delays Contractor from performing its obligations as set forth in the Agreement. Any modifications to Remote Access rights must be mutually agreed to in writing by County and Contractor.

### 2. Security Requirements

a. Contractor will not install any Remote Access capabilities on any County owned or managed system or network unless such installation and configuration is approved in writing by County's and Contractor's respective designees.

b. Contractor may only install and configure Remote Access capabilities on County systems or networks in accordance with industry standard protocols and procedures, which must be reviewed and approved by County's designee.

c. Contractor will only Remotely Access County systems, including access initiated from a County system, if the following conditions are met:

1. Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County requires advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.

2. Contractor Remote Access must include the following minimum control mechanisms:

   a. Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County site to Contractor site Virtual Private Network (VPN) infrastructure.

b. Centrally controlled authorizations (permissions) that are user specific (e.g., access lists that limit access to specific systems or networks).

c. Audit tools that create detailed records/logs of access attempts.

d. All Contractor systems used to Remotely Access County systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

e. Access must be established through a centralized collection of hardware and software centrally managed and controlled by County's and Contractor's respective designees.

### 3. Monitoring/Audit

County will monitor access to, and activities on, County owned or managed systems and networks, including all Remote Access attempts. Data on all activities will be logged on a County managed system and will include the date, time, and user identification.

### 4. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County IS unless otherwise stated in the Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in the Agreement.

### 5. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect County's data contained on County owned and/or managed systems and networks within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County networks or systems from non-County owned and/or managed networks or systems. Such access will be made in accordance with industry standard protocols and procedures as mutually agreed upon and will be approved in writing by County in a timely manner. Remote Access must include the control mechanisms noted in Paragraph 2.c.2 above.

### 6. Person Authorized to Act on Behalf of Parties

The following persons are the designees for purposes of this Agreement:

Contractor: Title/ Designee ________________________________

County: ______________________________________________

Either party may change the aforementioned names and or designees by providing the other party with no less than three (3) business day's prior written notice.

### 7. Remote Access Provisions

Contractor agrees to the following:

a. Only staff providing services or fulfilling Contractor obligations under the Agreement will be given Remote Access rights.

b. Any access to IS and/or County information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any other penalty allowed by law.

c. An encryption method reviewed and approved by the County will be used. County is solely responsible and liable for any delay or failure of County, as applicable, to approve the encryption method to be used by Contractor where such delay or failure causes Contractor to fail to meet or perform, or be delayed in meeting or performing, any of its obligations under the Agreement.

d. Contractor will be required to log all access activity to the County. These logs will be kept for a minimum of 90 days and be made available to County no more frequently than once every 90 days.

## 8. Remote Access Methods

a. All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County.

b. A Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

c. Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is inapplicable, please check the box marked N/A).

1. VPN Site-to-Site □ **Primary** □ **Backup** □ **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the vendor site and at the County, with a secure “tunnel” opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the designated software, devices and systems within the County, as specified above in Paragraph 1.b, from selected network-attached devices at the vendor site.

2. VPN Client Access □ **Primary** □ **Backup** □ **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

A CryptoCard will be issued to the Contractor in order to authenticate Contractor staff when accessing County IS via this method. The Contractor agrees to the following when issued a CryptoCard authentication device:

a. Because the CryptoCard allows access to privileged or confidential information residing on the County's IS, the Contractor agrees to treat the CryptoCard as it would a signature authorizing a financial commitment on the part of the Contractor.

b. The CryptoCard is a County-owned device, and will be labeled as such. The label must remain attached at all times.

c. The CryptoCard must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the CryptoCard will be kept under Contractor control.

e. The CryptoCard is issued to an individual employee of the Contractor and may only be used by the designated individual.

f. If the CryptoCard is misplaced, stolen, or damaged, the Contractor will notify County by phone within one (1) business day.

g. Contractor agrees to use the CryptoCard as part of its normal business operations and for legitimate business purposes only.

h. The CryptoCard will be issued to Contractor following execution of this Agreement. The CryptoCard will be returned to the County's designee within five (5) business days following contract termination, or upon written request of the County for any reason. Contractor will notify County's designee within one working day of any change in personnel affecting use and possession of the CryptoCard. Contractor will obtain the CryptoCard from any employee who no longer has a legitimate need to possess the CryptoCard. Lost or non-returned CryptoCards will be billed to the Contractor in the amount of $300 per card.

i. Contractor will not store password documentation or PINs with CryptoCards.

j. Contractor agrees that all employees, agents, contractors, and subcontractors who are issued the CryptoCard will be made aware of the responsibilities set forth in this Agreement in written form. Each person having possession of a CryptoCard will execute this Agreement where indicated below certifying that they have read and understood the terms of this Agreement.

3. County-Controlled VPN Client Access □ **Primary** □ **Backup** □ **N/A**

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the CryptoCard authentication token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes. When the Contractor needs to access County IS, the Contractor must first notify the County's designee.

The County's designee will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's IS. Contractor agrees to the following:

a. Because the PIN number allows access to privileged or confidential information residing on the County's IS, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.

b. The PIN number is confidential, County-owned, and will be identified as such.

c. The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.

e. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.

f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.

g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to IS and/or County data information that is not specifically authorized under the terms of this Agreement is prohibited and may result in contract termination and any other penalty allowed by law.

h. The PIN number will be issued to Contractor following execution of this Agreement.

i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

4. Manually Switched Dialup Modem □ **Primary** □ **Backup** □ **N/A**

Although not generally used, the Contractor may be provided Remote Access to County IS using a dialup modem. Contractor agrees to the following if using Switched Dialup Modem access:

a. Contractor will use reasonable efforts to notify the County's Technical Services Manager or designee at least ½ hour prior to access to allow County to activate the Switched Dialup Modem connection. Contractor will give the estimated time that the connection will be required, and specify when the access can be deactivated by County.

b. County acknowledges that Contractor may not be able to provide certain of its services (including, but not limited to, implementation services, maintenance and support (including Standard Support Services) and training services) using a Switched Dialup Modem connection.

c. County is solely responsible and liable for any inability or delay in Contractor performing its obligations under the Agreement where such inability or delay is caused by the use of a Switched Dialup Modem connection.

**Signatures of Contractor Employees receiving CryptoCards (if issued by County):**

CONTRACTOR: ______________________

___________________________________ [TYPE NAME HERE]

Date: ________________________________

[TITLE]

CONTRACTOR: ______________________

___________________________________ [TYPE NAME HERE]

Date: _______________________________

[TITLE]

CONTRACTOR: ______________________

___________________________________ [TYPE NAME HERE]

Date: ________________________________

[TITLE]

## APPENDIX B1 - FUNCTIONALITY AND INTEGRATION REQUIREMENTS RESPONSE FORM FOR A COUNTY HOSTED SOLUTION

Response Code: Offeror should place the appropriate letter designation in the “Availability” column according to the following codes and their description:

"A" means specification is one that currently exists in the proposed software, in the current production version and included in the County’s price.

"B" means specification is not in the proposed software but is a planned enhancement or will be added at no additional cost.

"C" means specification is not part of the proposed software but will be added at additional cost included in the County’s price. All such additional costs must be reported on cost response form.

"D" means specification is not available in the proposed software.

References: Please provide any additional information requested or any additional information useful to the proposal in the comments column. Please note some requirements explicitly request additional information on how a requirement is met and/or implemented. If referencing attachments or other included information, write the location(s) of where in your proposal (Section/Page Number) the requirement is addressed. Technical materials may be submitted as part of the proposal, and should be clearly labeled as such and may be referenced. References to web site URL’s or other on-line materials are not acceptable. If your availability response is “B” or “C”, please provide the estimated delivery date in the "Requirement Explanation/Comments" column below.

| ID | Functional/Technical Requirement | Priority Level (Critical / Highly Desirable / Desirable) | Availability | Requirement Explanation/Comments or Page and Binder Number in the proposal where additional information can be found. (Include delivery date if Availability is “B” or “C”) |
|---|---|---|---|---|
| | | | | |
| **Platform Support** | | | | |
| 1 | The proposed solution supports RIMM's Blackberry phone and tablet devices? | Highly Desirable | | |
| 2 | The proposed solution supports Apple iOS phone and tablet devices? | Critical | | Mandatory |
| 3 | The proposed solution supports Google Android phone and tablet devices? | Critical | | Mandatory |
| 4 | The proposed solution supports Microsoft Windows Mobile devices? | Desirable | | |
| 5 | The proposed solution supports Microsoft Windows Operating Systems (XP +)? | Desirable | | |
| 6 | The proposed solution supports Apple Mac OSX Operating Systems? | Desirable | | |
| 7 | The proposed solution will support Windows Phone 8 upon release? | Highly Desirable | | |
| 8 | Please list all other platforms the proposed solution supports? | | | |
| 9 | Please explain the typical time period before the proposed solution supports a new platform? | | | |
| 10 | Please explain what criteria is used to determine if a new platform will be supported? | | | |
| | | | | |
| | | | | |
| **Device Management - Core Features (Assumes Over-the-Air (OTA))** | | | | |
| | | | | |
| | **Platform Management - Agents** | | | |
| 11 | Does the proposed solution install an agent on the device, please explain? | | | |
| 12 | What is the proposed solution's agent resource consumption (memory, processor, footprint, etc.), please explain? | | | |
| 13 | What is the proposed solution's agent software lifecycle (how often is an update released for new functionality and/or patches)? | | | |
| 14 | Please list all past security vulnerabilities for the proposed solution's agent along with the time to release a patch? | | | |
| | | | | |
| | **Email Agents** | | | |
| 15 | Does the proposed solution require and utilize native mobile support from corporate email servers (Exchange ActiveSync, Blackberry Enterprise Server, Notes Traveler, etc.) to sync email content? Please explain | | | |
| 16 | The proposed solution does not conflict with or uninstall native email agents on device? | Highly Desirable | | |
| 17 | The proposed solution uses MDM API's available natively from vendors? Please list all of the vendor's embedded MDM API's you support. | Highly Desirable | | |
| 18 | The proposed solution vendor has signed MDM API agreements with vendors? | Highly Desirable | | |
| 19 | The proposed solution supports Open Mobile Alliance's Device Management policies? Please list. | Desirable | | |

| | | | | |
|---|---|---|---|---|
| | **Platform Management - Device** (Functions that verify and maintain platform policies and device management) | | | |
| 20 | The proposed solution provides capability to block external memory? | Critical | | |
| 21 | The proposed solution provides capability to run diagnostics? | Critical | | |
| 22 | The proposed solution provides capability to remote control (e.g., RDP-like capability) the device? | Desirable | | |
| 23 | The proposed solution provides capability to manage location support (e.g., GPS capability)? | Highly Desirable | | |
| 24 | The proposed solution provides capability to monitor battery life/cycle? | Desirable | | |
| 25 | The proposed solution provides capability to monitor performance? | Desirable | | |
| 26 | The proposed solution provides capability to manage device features (camera, WiFi, etc) | Critical | | |
| 27 | The proposed solution provides capability to perform device inventory? | Critical | | |
| 28 | The proposed solution provides capability to store configuration change history? | Desirable | | |
| 29 | The proposed solution provides capability to update device firmware? | Desirable | | |
| 30 | The proposed solution provides mobile asset tracking and management capability? | Highly Desirable | | |
| 31 | The proposed solution provides capability to backup devices? Please explain how this is implemented? | Critical | | |
| 32 | The proposed solution provides capability to recover/restore a device? Please explain how this is implemented? | Critical | | |
| 33 | The proposed solution provides capability to configure alerts to device/user? | Critical | | |
| | | | | |
| | **Device Provisioning/Enrollment** | | | |
| 34 | The proposed solution provides capability to enroll/provision devices using a self-service web portal? | Highly Desirable | | |
| 35 | The proposed solution provides capability to enroll/provision devices using a publicly available app? | Highly Desirable | | |
| 36 | The proposed solution provides capability to enroll/provision devices using a push method? | Desirable | | |
| 37 | The proposed solution provides capability to enroll/provision devices using an email notification? | Highly Desirable | | |
| 38 | Please list all other possible methods to enroll devices? | | | |
| 39 | Please explain device enrollment process? | | | |
| 40 | Please explain device enrollment authentication? | | | |
| | | | | |
| | **Application Management** (Functions that verify and maintain software policies) | | | |
| 41 | The proposed solution provides an app store feature? Please explain how this Is implemented. | Critical | | |
| 42 | The proposed solution provides capability to download and verify applications on device? | Critical | | |
| 43 | The proposed solution provides capability to manage enterprise (home grown) applications? | Critical | | |
| 44 | The proposed solution provides capability to white/black list enterprise or home grown applications? | Critical | | |
| 45 | The proposed solution provides capability to manage public applications? | Critical | | |
| 46 | The proposed solution provides capability to white/black list public applications? | Critical | | |
| 47 | The proposed solution provides capability to centrally deploy, update and patch applications? | Critical | | |
| 48 | The proposed solution provides capability to generate standard software/app deployment packages? | Highly Desirable | | |
| 49 | The proposed solution provides capability to quarantine applications? | Critical | | |
| 50 | The proposed solution provides capability to identify root/priviliged access applications? | Critical | | |
| 51 | The proposed solution provides capability to block public app stores? | Highly Desirable | | |
| 52 | The proposed solution provides capability to inventory applications both per device and globally? | Critical | | |
| | | | | |
| | **Security** (Functions that verify and maintain access, security and privacy policies) | | | |
| 53 | The proposed solution provides capability to configure access restrictions for NAC support? | Highly Desirable | | |
| 54 | The proposed solution provides capability to enforce passwords? | Critical | | |
| 55 | The proposed solution provides capability to enforce password complexity? | Critical | | |
| 56 | The proposed solution provides capability to enforce password retry limit with actions? | Critical | | |
| 57 | The proposed solution provides capability to enforce inactivity lock/timeout? | Critical | | |
| 58 | The proposed solution provides capability to enforce full device encryption(core encryption)? | Critical | | |
| 59 | The proposed solution provides capability to force device media encryption? | Critical | | |

| | | | | |
|---|---|---|---|---|
| 60 | Please describe how local data is secured? Please list all security and encryption methods used. | | | |
| 61 | Please describe how data in transit is secured? Please list all security and encryption methods used. | | | |
| 62 | The proposed solution provides capability to remotely lock devices? | Critical | | |
| 63 | The proposed solution provides capability to remotely unlock devices? Please explain how this is implemented? | Critical | | |
| 64 | The proposed solution provides capability to remotely wipe devices? | Critical | | |
| 65 | The proposed solution provides capability to remotely disable devices? | Critical | | |
| 66 | The proposed solution provides capability to authenticate users? | Critical | | |
| 67 | The proposed solution provides capability to authenticate devices? | Critical | | |
| 68 | The proposed solution provides capability to manage personal and corporate data separately? Please explain how this is accomplished. | Critical | | |
| 69 | The proposed solution provides containerization/sandboxing capability? | Highly Desirable | | |
| 70 | The proposed solution provides capability to selectively wipe (either personal or corporate) data in real-time without functional impact to devices? | Critical | | |
| 71 | The proposed solution provides capability to selectively wipe (either personal or corporate) data in real-time without requiring a device reboot? | Critical | | |
| 72 | The proposed solution provides firewall capability on device? | Critical | | |
| 73 | The proposed solution provides intrusion detection capability on device? | Desirable | | |
| 74 | The proposed solution provides anti-malware/virus capability on device? | Desirable | | |
| 75 | The proposed solution provides capability to secure configuration profiles? | Critical | | |
| 76 | The proposed solution provides capability for audit/trail logging device configuration changes including hardware and software? | Critical | | |
| 77 | The proposed solution provides real-time capability to audit/trail log device location (GPS Tracking) | Highly Desirable | | |
| 78 | The proposed solution provides detailed capability to audit/trail log web usage and breadcrumb mapping? | Desirable | | |
| 79 | The proposed solution provides capability to manage system level API's? | Desirable | | |
| 80 | The proposed solution provides capability to manage certificates (apply cert. to mail, WiFi, VPN, etc.? | Critical | | |
| 81 | The proposed solution provides capability to centrally manage WiFi 802.11 configuration? | Critical | | |
| 82 | The proposed solution provides capability to detect hacks (jailbreaking, rooting, rootkits) with configurable actions? Please explain how this is implemented? | Critical | | |
| 83 | The proposed solution provides capability to support VPN? | Critical | | |
| 84 | The proposed solution provides capability to manage port/interface access controls such as Bluetooth, Camera, USB, 3/4G, etc? | Critical | | |
| 85 | The proposed solution provides capablity to enforce min/max OS version? | Critical | | |
| 86 | The proposed solution provides S/MIME support? | Highly Desirable | | |
| 87 | The proposed solution provides capablity to push text (SMS) or SMTP (email) messages to devices from administration console? | Highly Desirable | | |
| 88 | The proposed solution provides capablity to manage cloud storage services such as iCloud, Skydrive, etc.? | Critical | | |
| 89 | The proposed solution provides capability to configure role-based policies? | Critical | | |
| 90 | The proposed solution provides capability to configure group-based policies? | Critical | | |
| | | | | |
| | | | | |
| **Device Management (Additional Features)** | | | | |
| 91 | The proposed solution offers mobile file management features? | Highly Desirable | | |
| 92 | The proposed solution offers mobile print management features? | Highly Desirable | | |
| 93 | The proposed solution offers mobile application development features? | Desirable | | |
| 94 | The proposed solution offers mobile identity management features? | Desirable | | |
| | | | | |
| | | | | |
| **Audit and Compliance** | | | | |
| 95 | The proposed solution provides capability to generate reports designed to satisfy standard compliance reporting? Please give brief examples relevant to government organizations (HIPAA, etc.) | Highly Desirable | | |
| 96 | The prosposed solution provides capability to generate warnings to users requiring them to take a configurable action? | Desirable | | |
| 97 | The prosposed solution provides capability to configure an auto-lock on the device if it has not checked in within a specified time limit? | Critical | | |
| | | | | |
| | **Secure lock and wipe functionality** | | | |
| 98 | Please list the min/max time required to initiate a remote lock or wipe? | | | |
| 99 | The proposed solution provides confirmation when the administrator console issues a lock or wipe command and successfully completes the command? | Critical | | |
| 100 | The proposed solution provides confirmation when the device passes a threshold for login attempts? | Critical | | |

| | | | | |
|---|---|---|---|---|
| 101 | The proposed solution provides confirmation when the device passes a time limit of being out of contact with the server? | Highly Desirable | | |
| 102 | The proposed solution provides geofencing capability with confirmation if the device passes a threshold for location. | Desirable | | |
| 103 | The proposed solution provides capability to confirm and notify administrators of user-initiated compliance errors (i.e., user installs banned/black listed app)? | Desirable | | |
| 104 | The proposed solution provides documentation on how it's methods will hold up against legal standards for data destruction? | Highly Desirable | | |
| 105 | The proposed solution's vendor has working relationships with forensic analysis vendors? Please explain. | Desirable | | |
| | | | | |
| | | | | |
| **Central Management** | | | | |
| 106 | Please list all OS platforms supported by your management server(s)? | | | |
| 107 | The proposed solution supports a dedicated local interface management UI? | Critical | | |
| 108 | The proposed solution supports a web browser management UI? | Desirable | | |
| 109 | The proposed solution supports an MMC snap-in management UI? | Desirable | | |
| 110 | The proposed solution supports a Microsoft System Center (SCCM) management UI? | Desirable | | |
| 111 | The proposed solution supports a CA service management UI? | Desirable | | |
| 112 | The proposed solution's central management server includes the ability to centrally manage MDM licenses on multiple gateways? | Desirable | | |
| 113 | Please list all steps the proposed solution takes to harden access to user backups, credentials, keys and policies stored on the management server? | | | |
| 114 | Please list all interface connections made between the management server and other systems within an enterprise (database, directory, etc.). For each connection please also list if the connection is secure or exposed during transit. | | | |
| 115 | Please explain how the proposed solution can be configured to provide high availability? | | | |
| 116 | The proposed solution provides capability to configure text (SMS) and SMTP (email) alerts from central management to administrators? | Critical | | |
| | | | | |
| | **Service Management** (telecom expense management (TEM)) | | | |
| 117 | The proposed solution provides capability to manage telecom related invoices? | Desirable | | |
| 118 | The proposed solution provides capability to manage telecom related contracts? | Desirable | | |
| 119 | The proposed solution provides capability to manage telecom mobile service usage monitoring and alerting? | Desirable | | |
| 120 | The proposed solution provides user self-service administration capability? | Desirable | | |
| | | | | |
| | **Directory Support** (Please indicate if the connection is read or write) | | | |
| 121 | The proposed solution supports Microsoft Active Directory services (AD)? | Critical | | |
| 122 | The proposed solution supports Lightweight Directory Access Protocol (LDAP)? | Critical | | |
| 123 | The proposed solution supports Novell Directory Services (NDS)? | Desirable | | |
| 124 | The proposed solution supports Remote Access Dial-in User Service (RADIUS)? | Desirable | | |
| 125 | The proposed solution supports multiple directories? | Critical | | |
| 126 | The proposed solution supports multiple directories in a multi-tenant configuration? | Critical | | |
| | | | | |
| | **Enterprise Support & Integration** | | | |
| 127 | The proposed solution can manage or integrate with non-native enterprise app stores? | Highly Desirable | | |
| 128 | The proposed solution supports Microsoft Office 365? Please explain how this is implemented? | Critical | | Mandatory |
| 129 | The proposed solution supports enterprise PKI (local CA, cryptography) systems? | Highly Desirable | | |
| 130 | The proposed solution integrates with enterprise systems management and monitoring solutions (Microsoft SCCM, SCOM, etc)? | Highly Desirable | | |
| 131 | The proposed solution integrates with on/off premise enterprise collaboration systems (SharePoint, Accellion, DropBox, etc)? | Highly Desirable | | |
| 132 | The proposed solution supports enteprise security systems including VPN, NAP/NAC systems (Cisco, Juniper, Citrix, UAG)? | Highly Desirable | | |
| 133 | The proposed solution supports enterprise data loss prevention systems (Microsoft RMS, Gigatrust)? | Desirable | | |
| | | | | |
| | | | | |
| **Operations and Technical Support/Help Desk** | | | | |
| 134 | As separate document, please provide sample outline-level implementation plan examples of your recommendations for preparation and installation. | | | |
| 135 | Please list all the technical support contact methods/options and hours available for administrators? | | | |
| 136 | The proposed solution provides technical support levels 1-3? | Critical | | |
| 137 | The proposed solution provides administrator self-service support? | Desirable | | |
| 138 | The proposed solution provides user self-service support? | Desirable | | |

| | | | | |
|---|---|---|---|---|
| 139 | The proposed solution provides capability to reset user credentials when locked out of device? Please describe all available methods with steps necessary to perform the reset/unlock. | Highly Desirable | | |
| | | | | |
| | | | | |
| **Multiple Users (Shared devices)** | | | | |
| 140 | The proposed solution provides support for dual-boot configurations? Please give examples. | Desirable | | |
| 141 | Please describe how your product may allow several people to share access to a device, and to have both common and segregated data areas. Ideally, this could be done without a reboot. | Desirable | | |
| 142 | Please describe your compatibility with virtual machine (VM) environments, including any special features or enhancements that are designed for virtual environments. List supported VM products. | Desirable | | |

## APPENDIX B2 - FUNCTIONALITY AND INTEGRATION REQUIREMENTS RESPONSE FORM FOR AN ASP (VENDOR HOSTED) SOLUTION

Response Code: Offeror should place the appropriate letter designation in the “Availability” column according to the following codes and their description:

"A" means specification is one that currently exists in the proposed software, in the current production version and included in the County’s price.

"B" means specification is not in the proposed software but is a planned enhancement or will be added at no additional cost.

"C" means specification is not part of the proposed software but will be added at additional cost included in the County’s price. All such additional costs must be reported on cost response form.

"D" means specification is not available in the proposed software.

References: Please provide any additional information requested or any additional information useful to the proposal in the comments column. Please note some requirements explicitly request additional information on how a requirement is met and/or implemented. If referencing attachments or other included information, write the location(s) of where in your proposal (Section/Page Number) the requirement is addressed. Technical materials may be submitted as part of the proposal, and should be clearly labeled as such and may be referenced. References to web site URL’s or other on-line materials are not acceptable. If your availability response is “B” or “C”, please provide the estimated delivery date in the "Requirement Explanation/Comments" column below.

| ID | Functional/Technical Requirement | Priority Level (Critical / Highly Desirable / Desirable) | Availability | Requirement Explanation/Comments or Page and Binder Number in the proposal where additional information can be found. (Include delivery date if Availability is “B” or “C”) |
|---|---|---|---|---|
| | | | | |
| **Platform Support** | | | | |
| 1 | The proposed solution supports RIMM's Blackberry phone and tablet devices? | Highly Desirable | | |
| 2 | The proposed solution supports Apple iOS phone and tablet devices? | Critical | | Mandatory |
| 3 | The proposed solution supports Google Android phone and tablet devices? | Critical | | Mandatory |
| 4 | The proposed solution supports Microsoft Windows Mobile devices? | Desirable | | |
| 5 | The proposed solution supports Microsoft Windows Operating Systems (XP +)? | Desirable | | |
| 6 | The proposed solution supports Apple Mac OSX Operating Systems? | Desirable | | |
| 7 | The proposed solution will support Windows Phone 8 upon release? | Highly Desirable | | |
| 8 | Please list all other platforms the proposed solution supports? | | | |
| 9 | Please explain the typical time period before the proposed solution supports a new platform? | | | |
| 10 | Please explain what criteria is used to determine if a new platform will be supported? | | | |
| | | | | |
| | | | | |
| **Device Management - Core Features (Assumes Over-the-Air (OTA))** | | | | |
| | | | | |
| | **Platform Management - Agents** | | | |
| 11 | Does the proposed solution install an agent on the device, please explain? | | | |
| 12 | What is the proposed solution's agent resource consumption (memory, processor, footprint, etc.), please explain? | | | |
| 13 | What is the proposed solution's agent software lifecycle (how often is an update released for new functionality and/or patches)? | | | |
| 14 | Please list all past security vulnerabilities for the proposed solution's agent along with the time to release a patch? | | | |
| | | | | |
| | **Email Agents** | | | |
| 15 | Does the proposed solution require and utilize native mobile support from corporate email servers (Exchange ActiveSync, Blackberry Enterprise Server, Notes Traveler, etc.) to sync email content? Please explain | | | |
| 16 | The proposed solution does not conflict with or uninstall native email agents on device? | Highly Desirable | | |
| 17 | The proposed solution uses MDM API's available natively from vendors? Please list all of the vendor's embedded MDM API's you support. | Highly Desirable | | |
| 18 | The proposed solution vendor has signed MDM API agreements with vendors? | Highly Desirable | | |

| | | | | |
|---|---|---|---|---|
| 19 | The proposed solution supports Open Mobile Alliance's Device Management policies? Please list. | Desirable | | |
| | | | | |
| | **Platform Management - Device** (Functions that verify and maintain platform policies and device management) | | | |
| 20 | The proposed solution provides capability to block external memory? | Critical | | |
| 21 | The proposed solution provides capability to run diagnostics? | Critical | | |
| 22 | The proposed solution provides capability to remote control (e.g., RDP-like capability) the device? | Desirable | | |
| 23 | The proposed solution provides capability to manage location support (e.g., GPS capability)? | Highly Desirable | | |
| 24 | The proposed solution provides capability to monitor battery life/cycle? | Desirable | | |
| 25 | The proposed solution provides capability to monitor performance? | Desirable | | |
| 26 | The proposed solution provides capability to manage device features (camera, WiFi, etc) | Critical | | |
| 27 | The proposed solution provides capability to perform device inventory? | Critical | | |
| 28 | The proposed solution provides capability to store configuration change history? | Desirable | | |
| 29 | The proposed solution provides capability to update device firmware? | Desirable | | |
| 30 | The proposed solution provides mobile asset tracking and management capability? | Highly Desirable | | |
| 31 | The proposed solution provides capability to backup devices? Please explain how this is implemented? | Critical | | |
| 32 | The proposed solution provides capability to recover/restore a device? Please explain how this is implemented? | Critical | | |
| 33 | The proposed solution provides capability to configure alerts to device/user? | Critical | | |
| | | | | |
| | **Device Provisioning/Enrollment** | | | |
| 34 | The proposed solution provides capability to enroll/provision devices using a self-service web portal? | Highly Desirable | | |
| 35 | The proposed solution provides capability to enroll/provision devices using a publicly available app? | Highly Desirable | | |
| 36 | The proposed solution provides capability to enroll/provision devices using a push method? | Desirable | | |
| 37 | The proposed solution provides capability to enroll/provision devices using an email notification? | Highly Desirable | | |
| 38 | Please list all other possible methods to enroll devices? | | | |
| 39 | Please explain device enrollment process? | | | |
| 40 | Please explain device enrollment authentication? | | | |
| | | | | |
| | **Application Management** (Functions that verify and maintain software policies) | | | |
| 41 | The proposed solution provides an app store feature? Please explain how this Is implemented. | Critical | | |
| 42 | The proposed solution provides capability to download and verify applications on device? | Critical | | |
| 43 | The proposed solution provides capability to manage enterprise (home grown) applications? | Critical | | |
| 44 | The proposed solution provides capability to white/black list enterprise or home grown applications? | Critical | | |
| 45 | The proposed solution provides capability to manage public applications? | Critical | | |
| 46 | The proposed solution provides capability to white/black list public applications? | Critical | | |
| 47 | The proposed solution provides capability to centrally deploy, update and patch applications? | Critical | | |
| 48 | The proposed solution provides capability to generate standard software/app deployment packages? | Highly Desirable | | |
| 49 | The proposed solution provides capability to quarantine applications? | Critical | | |
| 50 | The proposed solution provides capability to identify root/priviliged access applications? | Critical | | |
| 51 | The proposed solution provides capability to block public app stores? | Highly Desirable | | |
| 52 | The proposed solution provides capability to inventory applications both per device and globally? | Critical | | |
| | | | | |
| | | | | |
| | **Security** (Functions that verify and maintain access, security and privacy policies) | | | |
| 53 | The proposed solution provides capability to configure access restrictions for NAC support? | Highly Desirable | | |
| 54 | The proposed solution provides capability to enforce passwords? | Critical | | |
| 55 | The proposed solution provides capability to enforce password complexity? | Critical | | |

| | | | | |
|---|---|---|---|---|
| 56 | The proposed solution provides capability to enforce password retry limit with actions? | Critical | | |
| 57 | The proposed solution provides capability to enforce inactivity lock/timeout? | Critical | | |
| 58 | The proposed solution provides capability to enforce full device encryption(core encryption)? | Critical | | |
| 59 | The proposed solution provides capability to force device media encryption? | Critical | | |
| 60 | Please describe how local data is secured? Please list all security and encryption methods used. | | | |
| 61 | Please describe how data in transit is secured? Please list all security and encryption methods used. | | | |
| 62 | The proposed solution provides capability to remotely lock devices? | Critical | | |
| 63 | The proposed solution provides capability to remotely unlock devices? Please explain how this is implemented? | Critical | | |
| 64 | The proposed solution provides capability to remotely wipe devices? | Critical | | |
| 65 | The proposed solution provides capability to remotely disable devices? | Critical | | |
| 66 | The proposed solution provides capability to authenticate users? | Critical | | |
| 67 | The proposed solution provides capability to authenticate devices? | Critical | | |
| 68 | The proposed solution provides capability to manage personal and corporate data separately? Please explain how this is accomplished. | Critical | | |
| 69 | The proposed solution provides containerization/sandboxing capability? | Highly Desirable | | |
| 70 | The proposed solution provides capability to selectively wipe (either personal or corporate) data in real-time without functional impact to devices? | Critical | | |
| 71 | The proposed solution provides capability to selectively wipe (either personal or corporate) data in real-time without requiring a device reboot? | Critical | | |
| 72 | The proposed solution provides firewall capability on device? | Critical | | |
| 73 | The proposed solution provides intrusion detection capability on device? | Desirable | | |
| 74 | The proposed solution provides anti-malware/virus capability on device? | Desirable | | |
| 75 | The proposed solution provides capability to secure configuration profiles? | Critical | | |
| 76 | The proposed solution provides detailed capability for audit/trail logging device configuration changes including hardware and software? | Critical | | |
| 77 | The proposed solution provides real-time capability to audit/trail log device location (GPS Tracking) | Highly Desirable | | |
| 78 | The proposed solution provides detailed capability to audit/trail log device web usage (breadcrumb trails/mapping)? | Desirable | | |
| 79 | The proposed solution provides capability to manage system level API's? | Desirable | | |
| 80 | The proposed solution provides capability to manage certificates (apply cert. to mail, WiFi, VPN, etc.? | Critical | | |
| 81 | The proposed solution provides capability to centrally manage WiFi 802.11 configuration? | Critical | | |
| 82 | The proposed solution provides capability to detect hacks (jailbreaking, rooting, rootkits) with configurable actions? Please explain how this is implemented? | Critical | | |
| 83 | The proposed solution provides capability to support VPN? | Critical | | |
| 84 | The proposed solution provides capability to manage port/interface access controls such as Bluetooth, Camera, USB, 3/4G, etc? | Critical | | |
| 85 | The proposed solution provides capablity to enforce min/max OS version? | Critical | | |
| 86 | The proposed solution provides S/MIME support? | Highly Desirable | | |
| 87 | The proposed solution provides capablity to push text (SMS) or SMTP (email) messages to devices from administration console? | Highly Desirable | | |
| 88 | The proposed solution provides capablity to manage cloud storage services such as iCloud, Skydrive, etc.? | Critical | | |
| 89 | The proposed solution provides capability to configure role-based policies? | Critical | | |
| 90 | The proposed solution provides capability to configure group-based policies? | Critical | | |
| | | | | |
| | | | | |
| **Device Management (Additional Features)** | | | | |
| 91 | The proposed solution offers mobile file management features? Please explain how this is implemented? | Highly Desirable | | |
| 92 | The proposed solution offers mobile print management features? Please explain how this is implemented? | Highly Desirable | | |
| 93 | The proposed solution offers mobile application development features? | Desirable | | |
| 94 | The proposed solution offers mobile identity management features? | Desirable | | |
| | | | | |
| | | | | |
| **Audit and Compliance** | | | | |
| 95 | The proposed solution provides capability to generate reports designed to satisfy standard compliance reporting? Please give brief examples relevant to government organizations (HIPAA, etc.) | Highly Desirable | | |
| 96 | The prosposed solution provides capability to generate warnings to users requiring them to take a configurable action? | Desirable | | |
| 97 | The prosposed solution provides capability to configure an auto-lock on the device if it has not checked in within a specified time limit? | Critical | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | **Secure lock and wipe functionality** | | | |
| 98 | Please list the min/max time required to initiate a remote lock or wipe? | | | |
| 99 | The proposed solution provides confirmation when the administrator console issues a lock or wipe command and successfully completes the command? | Critical | | |
| 100 | The proposed solution provides notification when the device passes a threshold for login attempts? | Critical | | |
| 101 | The proposed solution provides notification when the device passes a time limit of being out of contact with the server? | Highly Desirable | | |
| 102 | The proposed solution provides geofencing capability with notification if the device passes a threshold for location. | Desirable | | |
| 103 | The proposed solution provides capability to confirm and notify administrators of user-initiated compliance errors (i.e., user installs banned/black listed app)? | Desirable | | |
| 104 | The proposed solution provides documentation on how it's methods will hold up against legal standards for data destruction? | Highly Desirable | | |
| 105 | The proposed solution's vendor has working relationships with forensic analysis vendors? Please explain. | Desirable | | |
| | | | | |
| | | | | |
| **Central Management** | | | | |
| | | | | |
| 106 | The proposed solution supports a dedicated local interface management UI? | Critical | | |
| 107 | The proposed solution supports a web browser management UI? | Desirable | | |
| 108 | The proposed solution supports an MMC snap-in management UI? | Desirable | | |
| 109 | The proposed solution supports a Microsoft System Center (SCCM) management UI? | Desirable | | |
| 110 | The proposed solution supports a CA service management UI? | Desirable | | |
| 111 | The proposed solution's central management server includes the ability to centrally manage MDM licenses on multiple gateways? | Desirable | | |
| 112 | Please list all steps the proposed solution takes to harden access to user backups, credentials, keys and policies stored on the management server? | | | |
| 113 | Please list all interface connections made between the management server and other systems within an enterprise (database, directory, etc.). For each connection please also list if the connection is secure or exposed during transit. | | | |
| 114 | Please explain how the proposed solution provides high availability? | | | |
| 115 | The proposed solution provides capability to configure text (SMS) and SMTP (email) alerts from central management to administrators? | Critical | | |
| | | | | |
| | **Service Management** (telecom expense management (TEM)) | | | |
| 116 | The proposed solution provides capability to manage telecom related invoices? | Desirable | | |
| 117 | The proposed solution provides capability to manage telecom related contracts? | Desirable | | |
| 118 | The proposed solution provides capability to manage telecom mobile service usage monitoring and alerting? | Desirable | | |
| 119 | The proposed solution provides user self-service administration capability? | Desirable | | |
| | | | | |
| | **Directory Support** (Please indicate if the connection is read or write) | | | |
| 120 | The proposed solution supports Microsoft Active Directory services (AD)? | Critical | | |
| 121 | The proposed solution supports Lightweight Directory Access Protocol (LDAP)? | Critical | | |
| 122 | The proposed solution supports Novell Directory Services (NDS)? | Desirable | | |
| 123 | The proposed solution supports Remote Access Dial-in User Service (RADIUS)? | Desirable | | |
| 124 | The proposed solution supports multiple directories? | Critical | | |
| 125 | The proposed solution supports multiple directories in a multi-tenant configuration? | Critical | | |
| | | | | |
| | **Enterprise Support & Integration** | | | |
| 126 | The proposed solution can manage or integrate with non-native enterprise app stores? | Highly Desirable | | |
| 127 | The proposed solution supports Microsoft Office 365? Please explain how this is implemented? | Critical | | Mandatory |
| 128 | The proposed solution supports enterprise PKI (local CA, cryptography) systems? | Highly Desirable | | |
| 129 | The proposed solution integrates with enterprise systems management and monitoring solutions (Microsoft SCCM, SCOM, etc)? | Highly Desirable | | |
| 130 | The proposed solution integrates with on/off premise enterprise collaboration systems (SharePoint, Accellion, DropBox, etc)? | Highly Desirable | | |
| 131 | The proposed solution supports enteprise security systems including VPN, SSL, NAP/NAC systems (Cisco, Juniper, Citrix, UAG)? | Highly Desirable | | |
| 132 | The proposed solution supports enterprise data loss prevention systems (Microsoft RMS, Gigatrust)? | Desirable | | |
| | | | | |
| | | | | |
| **Operations and Technical Support/Help Desk** | | | | |
| 133 | As separate document, please provide sample outline-level implementation plan examples of your recommendations for preparation and installation. | | | |

| | | | | |
|---|---|---|---|---|
| 134 | Please list all the technical support contact methods/options and hours available for administrators? | | | |
| 135 | The proposed solution provides technical support levels 1-3? | Critical | | |
| 136 | The proposed solution provides administrator self-service support? | Desirable | | |
| 137 | The proposed solution provides user self-service support? | Desirable | | |
| 138 | The proposed solution provides online service status monitoring? | Highly Desirable | | |
| 139 | The proposed solution provides capability to reset user credentials when locked out of device? Please describe all available methods with steps necessary to perform the reset/unlock. | Highly Desirable | | |
| | | | | |
| | | | | |
| **Multiple Users (Shared devices)** | | | | |
| 140 | The proposed solution provides support for dual-boot configurations? Please give examples. | Desirable | | |
| 141 | Please describe how your product may allow several people to share access to a device, and to have both common and segregated data areas. Ideally, this could be done without a reboot. | Desirable | | |
| 142 | Please describe your compatibility with virtual machine (VM) environments, including any special features or enhancements that are designed for virtual environments. List supported VM products. | Desirable | | |
| | | | | |
| | | | | |
| **ASP/Vendor Hosted/Cloud General** | | | | |
| 143 | The proposed solution is FISMA certified/compliant? | Critical | | |
| 144 | The proposed solution is ISO/IEC certified/compliant? | Desirable | | |
| 145 | The proposed solution is SAS-70 or equivalent certified/compliant? | Critical | | |
| 146 | The proposed solution is HIPAA certified/compliant? | Critical | | |
| 147 | The proposed solution is hosted completely in the Continental US (CONUS)? | Critical | | |
| 148 | Please list all interface connections made between vendor hosted solution (off premise) and a customer enterprise (on premise). For each connection please list if and how the connection is secure or exposed during transit. | | | |
| 149 | The proposed solution is not reliant on a single geographically located data center for operations (single point of failure). Please provide and explain a high-level architecture on how this is implemented. | Critical | | |

# Question and Answers for Bid #RFP-PRO-FY13-0009 - Mobile Device Management System

**OVERALL BID QUESTIONS**

**There are no questions associated with this bid. If you would like to submit a question, please click on the "Create New Question" button below.**

**Question Deadline: Aug 2, 2012 3:00:00 PM PDT**