County of Santa Clara
Office of the County Executive
Procurement Department
2310 N. First Street Suite 201
San Jose, CA 95131-1040
Telephone 408-491-7400 • Fax 408-491-7496

AGREEMENT BETWEEN THE COUNTY OF SANTA CLARA AND ALERTUS TECHNOLOGIES, LLC FOR GOODS AND RELATED SERVICES

This Agreement is entered into by and between the County of Santa Clara (the "County") and Alertus Technologies, LLC. ("Contractor") (the "Agreement").

The effective date of the Agreement is November 20, 2014. The parties, intended to be bound, mutually agree as follows:

KEY PROVISIONS

AGREEMENT TITLE:	Emergency Management Notification Software
AGREEMENT NUMBER:	5500002508
INITIAL AWARD DATE:	November 26, 2014
AGREEMENT TERM:	November 26, 2014 through November 25, 2017, unless terminated earlier or otherwise amended, with option by County to renew for two additional one-year periods
COMMODITY NAME:	Computer Software (209) Software Maintenance (92045)
AUTHORIZED USER:	Santa Clara Valley Health and Hospital System 2325 Enborg Lane, San Jose, CA 95128
COUNTY DEPARTMENT CONTACT:	Bud Ramsey, (408) 793-6562 Bud.ramsey@hhs.sccgov.org
SUPPLIER:	Alertus Technologies, LLC 11785 Beltsville Rd., 15th Floor Beltsville, MD 20705
SUPPLIER CONTACT:	Peter Lester, (866) 425-3788 x706, plester@alertus.com Ben Brewer, (866) 425-3788, bbrewer@alertus.com
SUPPLIER NUMBER:	1036072
PURPOSE:	To establish a contract with Alertus Technologies, LLC for emergency management notification software

TAX STATUS:	Product taxable; Services Non-taxable
PAYMENT TERMS:	Net 30 Days
TOTAL AGREEMENT VALUE:	Not to Exceed **$59,750.**
COUNTY CONTRACT ADMINISTRATOR:	Alicia Jauregui, Alicia.jauregui@prc.sccgov.org, (408) 491-7480
EXHIBITS	The following Exhibits are attached hereto and incorporated herein by reference and constitute a material part of the Agreement:

Exhibit A – Price Summary

Exhibit B – Statement of Work

Exhibit C – Technical Requirements

Exhibit D – Features, Functionalities and Integration

Exhibit E – Service and Support

Exhibit F– County of Santa Clara Standard Terms and Conditions

Exhibit G – Alertus License and Support Agreement

Exhibit H – Insurance Requirements

Exhibit I – Vendor Remote Access Agreements

By signing below, signatory warrants and represents that he/she executed this Agreement in his/her authorized capacity, that he/she has the authority to bind the entity listed below to contractual obligations and that by his/her signature on this Agreement, the entity on behalf of which he/she acted, executed this Agreement.

COUNTY OF SANTA CLARA

12/1/14

Julie Toy Date
Procurement Manager

12/1/14

Jenti Vandertuig Date
Director of Procurement

APPROVED AS TO FORM AND LEGALITY

11/26/14

Robert Nakamae Date
Deputy County Counsel

CONTRACTOR

By: _____

Print: Jason Volk

Title: CEO

Date: 11/25/2014

EXHIBIT A
PRICE SUMMARY

Section I – One Time Costs

Name of Deliverable:	Description:	Fixed Price:
Alertus Notification System	Alertus Software Activation License (Perpetual)	$4,950.00 each
Alertus Desktop Notification	Alertus Desktop Client application licensing	7,000 each @ $3.40 each
	Customization	Included at no cost
	Installation/Implementation	Included at no cost
	Project Management	Included at no cost
	Training, including all materials	Included at no cost
	Travel Expenses	Included at no cost
	Applicable Sales Tax	N/A
	TOTAL ONE TIME COST:	$34,950.00

Section II – Recurring Annual Costs

MAINTENANCE AND SUPPORT	ANNUAL COST
Year One	No cost
Year Two	$6200
Year Three	$6200
Year Four	$6200
Year Five	$6200
TOTAL Years 1 – 5	$24,800

Maintenance and Support shall be paid net 30 days from anniversary date of each year and corrected invoice.

Optional Costs

ESCROW ACCOUNT	ANNUAL FEE
Year One	$500
Year Two	$500
Year Three	$500
Year Four	$500
Year Five	$500
TOTAL RECURRING COST	$2500

EXHIBIT B
STATEMENT OF WORK

Within 14 calendar days of commencement of the Agreement, both parties shall meet to finalize the Statement of Work (SOW). At a minimum, the final SOW shall include the following:

1. Assumptions;
2. All tasks to go-live, including training;
3. Roles and Responsibilities of both parties;
4. Timelines to complete tasks;
5. Deliverables;
6. Criteria for acceptance testing; and
7. Final Acceptance Criteria.

Both parties agree that the SOW shall be detailed and capture all work to be performed by the Contractor in order for the County to go-live. Contractor shall have staff readily available on day of go-live to provide service and support in case questions or issues with the software arises.

Once the SOW is finalized and signed by both parties, any additional work shall be contracted via a Change Notice to the SOW, which shall be agreed to by both parties, in writing. Any and all Change Notices to the SOW shall specifically identify the additional work to be done, the additional hours and the contracted rates. Any fees associated with the additional work is negotiable.

Any additional work and/or products purchased under this Agreement shall be within the scope of the emergency management software system. The final SOW and any and all Change Notices to the SOW shall be automatically incorporated into the Agreement by reference hereto. Change Notices with original signatures shall be submitted to the County Contract Administrator for record keeping. The SOW and Changes Notices may not contain language that replaces the Agreement terms and conditions. Agreement terms and conditions may only be revised via an Amendment to the Agreement and signed by both parties

EXHIBIT B
STATEMENT OF WORK

This Statement of Work ("SOW") is hereby effective at contract commencement "Effective Date") and shall be governed by the terms and conditions of the Agreement entered into between Alertus Technologies, LLC ("Supplier") and Santa Clara Valley Health and Hospital System and its Affiliates ("SCVHHS") effective November 26, 2014 ("Agreement"). Unless otherwise stated in this SOW, all defined terms shall have the meaning designated in the Agreement. If there are any conflicts between the provisions of this SOW and the Agreement, the terms of the Agreement shall control with respect to the subject matter of this SOW. Supplier shall provide the services described herein ("Services").

1. Background / Introduction:

SCVHHS has highlighted the need for a desktop alerting focused emergency notification system. The Alertus System proposed must be capable of operating in a hosted configuration with the Alertus Server hosted by Santa Clara County. The Alertus system must successfully transmit an alert to up to 7,000 desktop notification endpoints within 1-2 seconds of transmission initiation.

2. Scope of Services:

The Supplier shall deliver an Alertus System capable of meeting the SCVHHS Team's intent. The Alertus System shall be defined as: an Alertus Server deployed upon a Santa Clara County provided virtual or physical server; and the Alertus Desktop Client with 7,000 licenses. Upon receipt and acceptance of a purchase order for the above materials Alertus shall: work with SCVHHS to identify and validate a qualified host name for the Alertus Server; establish permissions for SCVHHS's primary point of contact (POC) to access the My Alertus Customer Portal; build Alertus Server and Alertus Desktop Client software based upon SCVHHS's identified network settings and issue same to SCVHHS's primary POC for download; consult with SCVHHS and its designees (e.g. Santa Clara County) as needed on Alertus Server provisioning, installation, and configuration; consult with SCVHHS as needed on Alertus Desktop Client application installation via SCVHHS's internal desktop management suite; provide administrative and or user familiarization training via webinar; and assist SCVHHS in testing system functionality as required during the initial period as the Alertus System transitions from implementation to support. Alertus shall not provide on-site consultation or installation services under the scope of this project.

Name of Deliverable:	Description of Deliverable:
Alertus Server Installation Package	Software installation file which accomplishes the installation and initial configuration of the Alertus Server software on the designated Santa Clara Valley Health and Hospital System's prepared physical or virtual server.
Alertus Desktop Client Installation Package	Software installation file which accomplishes the installation and initial configuration of the Alertus Server Desktop Client on Santa Clara Valley Health and Hospital System's network desktops via SCVHHS's internal desktop management processes.

EXHIBIT B
STATEMENT OF WORK

3. Delivery Schedule:

Overall Project Start Date:	Not yet defined
Overall Project Completion Date:	Not yet defined

Name of Deliverable:	Estimated Date of Delivery:
Alertus Server Installation Package	Not yet defined

Alertus Desktop Client Application Installation Package	Not yet defined

4. Key Supplier Personnel:

(List Supplier Personnel that are key individuals that should not be removed from the project without SCVHHS's written consent)

Name:	Title:	Email:
Ben Brewer	Director, Professional & Client Services	bbrewer@alertus.com
Rick Veader	Lead Support Analyst	rveader@alertus.com and support@alertus.com

5. Place of Performance: Alertus Technologies main offices located at 11785 Beltsville, MD 20705, and its remote operating location in Winchester, TN.

6. SCVHHS Property:

None known at this time.

7. Implementation Overview:

The following provides a high-level overview of the process Alertus Technologies undertakes on behalf of and in collaboration with the Alertus System Client.

The Implementation Process shall have three phases: Planning, Implementation and Cutover, and Support. Process duration and completion time shall be dependent upon the project scope.

The Planning phase shall commence with the receipt and acceptance of SCVHHS Purchase Order and shall involve the following activities led by the Alertus Implementation Manager:

a. Project scope review
b. Identify and resolve any scope questions
c. Determine the SCVHHS network settings required to advance the project to production ready

d. First Implementation Meeting with SCVHHS's Primary Point of Contact (POC) for introductions, process discussion, and providing the POC with the appropriate network settings form
e. SCVHHS POC(s) shall complete and return the form to Alertus Implementation Manager
f. Network settings shall be reviewed for suitability; identified issues shall be address with SCVHHS POC and resolved advancing order to production ready status
g. Validated network settings shall be applied to build Alertus Server and Alertus Desktop Client software
h. My Alertus Portal Access shall be created for SCVHHS POC; Alertus shall advise SCVHHS POC installation files are available for download
i. Production manager shall develop SCVHHS specific firmware and assemble any Alertus devices required by project scope; completed hardware shall be tested, packaged and shipped to SCVHHS POC

The Implementation and Cutover phase shall begin while aspects of the Planning Phase are completing (e.g. Alertus device manufacture) and shall consist of the following activities led by the Alertus Implementation Manager:

a. Consult with and assist SCVHHS POCs in provisioning the physical/virtual server, installation of Alertus Server software, and provisioning of any Alertus Desktop Client software
b. Consult with SCVHHS POCs on installation of Alertus device installation and implementation
c. Provide System Administrator and User training scoped to fit SCVHHS specific needs
d. Assist in implementation and testing of purchased integrations
e. Continue to work any scope aspects impacted by back order, custom development, etc.; order is not considered fulfilled until fully implemented

The Support phase begins immediately after installation and implementation of the Alertus Server and any Alertus endpoints (i.e. Alertus Desktop Client, Alert Beacons and other Alertus devices) and is not dependent upon completion of the Implementation and Cutover Phase

8. Implementation Process Responsibilities:

Milestones and timelines shall be agreed upon during the initial project planning call. The following provides a representation of responsibilities and notional timelines and is reflected in business days. These activities shall commence immediately following issuance and acceptance of a purchase order or other contract for the Alertus System.

a. Alertus Client Services personnel review Alertus System Scope and address any questions **(Day 1)**
b. Alertus Implementation Manager identifies and provides proper Alertus Network Settings Form to the Customer's Primary Contact **(Day 1)**
c. Alertus Production Manager reviews Order Information, validates equipment stock availability and orders any materials required to produce any hardware ordered **(Day 1)**
d. SCVHHS POC receives, reviews, and begins to complete the Alertus Network Settings Form

e. Alertus Implementation Manager serves as liaison with Customer to address Network Settings questions and facilitate timely return of the Network Settings Form **(Day 1)**
f. SCVHHS POC completes and returns the Alertus Network Settings Form to Implementations@alertus.com **(Day 1 + 3 to 5 days)**
g. Alertus Implementation Manager shall follow up with Customer POC a minimum of once every five (5) business days to ensure timely return of the Alertus Network Settings Form; if the Customer POC has not returned the network settings form after 15 business days, the Implementation Manager shall escalate to the Sales Account Manager for assistance **(Day 1 +5 to 15 days)**
h. Alertus Implementation Manager receives the completed Alertus Network Settings Form from the Customer; Production, Implementations, and Technical Support personnel review the network settings for completeness and suitability **(Network Settings Received + 1 Day)**
i. Alertus Implementation Manager addresses any network settings questions with SCVHHS POC **(Network Settings Received + 1 Day)**
j. Alertus Production Manager loads network settings into the Production Database which serves to create the software license, Alertus Server and Alertus Desktop Client configuration files, and creates Customer Portal Access and initiates an automated email to the SCVHHS POC with portal access and software download information **(Network Settings Accepted + 1 Day)**
k. SCVHHS identifies and provisions a server to host the Alertus Server software **(Day 1 + 5 to 10 days)**
l. Alertus provides Alertus System software installation and provisioning consultation support to SCVHHS POCs if required **(Network Settings Accepted + 2 to 10 Days)**
m. Alertus and SCVHHS discuss remote support access and implement if required **(Installation Complete + 1 Day)**
n. Alertus and SCVHHS schedule and conduct Alertus System training if required and adds appropriate comments to Order Stage Details **(Installation Complete + 5 to 10 Days)**
o. Alertus and SCVHHS complete Alertus System Acceptance Testing **(Training Complete + 2 to 3 Days)**
p. Alertus addresses/resolves and outstanding issues, retests as required **(Initial Testing Complete + 5 Days)**
q. Alertus and SCVHHS reaccomplish Alertus System Acceptance Testing if required
r. SCVHHS acknowledges Alertus System Acceptance
s. Implementation Process is complete

9. Alertus System Acceptance Testing

Alertus System Acceptance Testing is accomplished within the timeframe stated under the County's Terms and Conditions under #17.1. Acceptance Testing does not validate Alertus System user proficiency, but the Alertus System's ability to support required functionality, as stated under Exhibit B – Technical Requirements and Exhibit C – Features, Functionalities and Integration. Acceptance testing for an Alertus System for the stated scope shall include, at minimum, the following:

☐ SCVHHS Alertus System Administrators can access the Alertus Middleware
☐ Alertus System privileged user can successfully access the Alertus Console
☐ Alertus Server denies access to Alertus Console when invalid credentials are provided

- ☐ SCVHHS Alertus System Administrators can add, modify, delete user profiles
- ☐ SCVHHS Alertus privileged user can successfully create, modify, activate, and delete alert templates
- ☐ SCVHHS Alertus privileged user can successfully view reports
- ☐ SCVHHS Alertus System Administrators can successfully access System Configuration
- ☐ The Alertus Desktop Client Activation application successfully starts after installation, registers with the Alertus Server, pulls alert data from the Alertus Server, and populates a desktop notification

10. System Documentation

a. Documentation during installation shall be provided by email, webinar and via access to the Alertus customer support Portal web site. All documentation shall available in a searchable format and updated regularly in the customer support portal.
b. Detailed System Administrator documentation (electronic) shall be provided via access to the Alertus customer support portal web site. This information shall be updated and accessible to all administrators. Information is organized by role and well indexed (e.g. sustainment documentation).

11. Reports

a. The Contractor's report application shall be available from the Reports Menu under AlertusWeb.
b. The following reports shall be available, which include, but are not limited to:

   i. Alert History – shall generate a history of the last 20 alerts that were dispatched by Alertus System, including both alerts sent through AlertusWeb and via integrated 3rd party applications.
   ii. Device Acknowledgement – shall generate a report with a summary of alert devices acknowledgement information for a selected alert. This shall include various acknowledgement summary metrics, graphical charts and individual device acknowledgement times.
   iii. Device Activation – shall generate a report with a summary of alert device activation information for the selected alert. This shall include various activation performance metrics, graphical charts and individual device activation times.
   iv. Group Membership – shall generate a report of alert device membership by group.
   v. Location Membership – shall generate a report of alert device memberships by location.
   vi. View Device Status – shall generate a report that shall provide an overview of the current system status. This shall allow for verification of system performance and identification of connectivity issues.

12. Risk Management

Consequence	Failure	Production Impact
Minor	Network settings not identified within five (5) business days of order	Application build proves delayed; minor schedule adjustment
Moderate	Alertus System application builds are incorrect	Requires rescission of application builds, revalidation of network

		settings, and renewed Alertus System application builds
Moderate	Server provisioning not completed	Delays installation and configuration of Alertus Server software and introduces delays to training and acceptance testing.
Moderate	Alertus Desktop Client application provision and push across network not completed.	Delays training and acceptance testing.
Moderate	Training not completed in accordance with project plan milestones	Delays acceptance testing.
[redacted]	[redacted]	[redacted]

Risk Rating	Required Actions	Approvals
Minor	Risk assessed and addressed by Implementation Engineer and Client system POC.	Project Manager
Moderate	Risk assessed by Director Client Services and Client Project/Program Manager; remedies identified and implemented.	Director/PM
[redacted]	[redacted]	[redacted]

13. Project Management Team

a. Led by the Director of Professional Services, Contractor shall utilize an evolving PMO approach to continually fine-tune how it delivers products/solutions to consistently exceed customer goals. Each project has an internal organizational matrix that outlines the roles and responsibilities of project leaders. By doing so, it demonstrates the benefits of the recommended changes while fine-tuning the process.

b. Project Team:

POSITION	NAME/TITLE	RESPONSIBILITIES
Leader	Ben Brewer, Director of Professional Services	Overall responsibility for Alertus project deliverables
Director of Technical Assurance	Blake Robertson, CTO	Overall responsibilities for technical compliance and performance
Technical Support 1	Rick Veader	Overall responsibility for configuration and training
Technical Support 2	Gary El-Gamil	Overall responsibility for software implementation
Technical Support 3	Philip Anderson	Overall responsibility for hardware implementation (if applicable, extended notification)
Account Manager	Peter Lester	On-going responsibilities for account satisfaction

c. Contractor shall provide a variety of ways to publicize the system including:

i. PDFs
ii. Overview webinars
iii. All relevant Santa Clara personnel shall be given access to our customer support portal website, which provides information on the Alertus Desktop Notification and all the other features / endpoints of the total enterprise wide alerting solution;
iv. Contractor shall provide hands-on (webinar) assistance with initial implementation/configuration (templates, groups, etc.) through completion of initial testing whereas the system shall be ready for use.

d. Organizing Support Infrastructure and Processes

i. Contractor personnel shall confer with appropriate County personnel to capture details and specifications of current systems (hardware/software) in place;
ii. Coordinate with schedules to meet targeted timeframes including software install, initial configuration, fixing any issues necessary to meet agreed to "go live date".

e. Consulting on content / set up / management
This shall be an on-going activity that begins day one and carries through successful launch of the application

1. Contractor personnel shall interface with the appropriate staff of the County, and hospital. The Project Leader shall collect all key contacts and roles. All such County personnel shall be entered into Contractor's CRM along with contact information for full access to the Alertus Support Team. The Technical Support lead shall take charge of software install, configuration consulting and training. The Alertus Project Leader shall oversee the delivery. The Account Manager shall be the point of escalation. Lastly, while under contract, any such County personnel may receive access to Customer Support Portal and technical assistance simply via emailing support@alertus.com.

2. The County shall provide contact information for their Project Manager assigned to this project. Additionally, the same applies to providing Alertus the technical point of contact for this project. Such person(s) shall have the authority to, among others, being able to provision a server that shall store the Alertus software, be able to provide VPN access to the server or onsite access, provide a DNS host name for server ID, directly be able to, or cause to, distribute/image the Contractor provided client software to desired PCs, be available, or cause another to be available, for initial configuration and testing through successful launch.

3. The Alertus Project Leader shall be the primary contact for project related questions, coordination and concerns. Throughout the project the Project Leader shall coordinate access to the appropriate resources at Alertus to complete the install and testing. This shall be accomplished with a series of project management calls, information forms and one-on-one sessions with an assigned Alertus engineer.

EXHIBIT B
STATEMENT OF WORK
Implementation Checklist

Successfully deploying an emergency notification system across an organization requires coordination between different departments and resources. To facilitate this process we've put together the following checklist to assist you with setting up your Alertus system! Complete the applicable sections for your implementation.

Key: BO = Business Owner; IT = IT System Admin; NW = IT Network Admin; ■ = Hardware Installer; Documentation *link*

A. Getting Started Tasks

--All Alertus Servers—

1. Review the Alertus Support documentation BO IT NW ■ http://support.alertus.com
2. Click "Sign up With Us" and sign up with your email address
3. Go To https://helpdesk.alertus.com/support/discussions/topics/20119 to subscribe to Major Alertus software updates
4. Decide on an Alertus Hostname BO NW http://support.alertus.com/wiki/Hostname
5. Email completed Network Settings Form to support@alertus.com NW IT
6. Primary POC receives credentials to access https://my.alertus.com customer download portal *--via email from* support@alertus.com-- BO
7. Provision a physical or virtual server for your Alertus installation satisfying the following specs: http://support.alertus.com/wiki/Server_System_Requirements IT
8. Create a DNS record for your Alertus Hostname that points to your provisioned server NW IT
9. Plan how you shall use Alertus to communicate during an emergency BO IT
10. Determine scenarios where you need to communicate using Alertus
11. Determine if alerts shall always be sent to all devices or if they shall be targeted to specific buildings, floors, campuses, geographic regions, or other recipient groups
12. Decide if alerts shall be initiated from Alertus or a 3rd party partner.
13. Determine who shall be responsible for activating the Alertus System
14. Decide on Alertus behavior for each scenario

B. Server Configuration Tasks

--All Alertus Servers—

1. Install the Alertus Server package IT http://support.alertus.com/wiki/Server_Install
2. Login to the Alertus Web Console BO
   Default Credentials
   Username = admin
   Password = admin
3. Change the default admin password to a secure choice BO
4. Configure Groups BO http://support.alertus.com/wiki/Groups
5. Configure Profiles BO http://support.alertus.com/wiki/Alert_Profiles
6. Configure Message Templates BO http://support.alertus.com/wiki/Message_Templates
7. Configure Presets BO http://support.alertus.com/wiki/Preset_Alert
8. Configure global defaults BO http://support.alertus.com/wiki/AlertusWeb_Settings

9. Create user roles / restrictions to meet user control needs BO
   http://support.alertus.com/wiki/AlertusWeb_User_Accounts
10. Configure email settings *--recommended but optional--* IT
    http://support.alertus.com/wiki/Server_Configuration
11. Configure SSL certificate *--recommended but optional--* IT
    http://support.alertus.com/wiki/Accessing_AlertusWeb_through_HTTPS_%28_SSL_%29
12. Configure monitoring *--recommended but optional--* IT BO
    http://support.alertus.com/wiki/Monitoring
    http://support.alertus.com/wiki/Notification_and_Monitoring
13. Configure backup / restore *--recommended but optional--* IT
    http://support.alertus.com/wiki/Server_Backup_Restore
14. Configure LDAP/AD for user authentication *--optional--* IT
    http://support.alertus.com/wiki/LDAP
15. Configure NOAA/other threatwatcher feeds *--optional--* IT BO
    http://support.alertus.com/wiki/ThreatWatcher
16. Configure 3rd party integrations if applicable *--optional--* NW IT BO
    http://support.alertus.com/wiki/API_Integration

C. Alertus Desktop Client Tasks

--Skip if you did not purchase Alertus Desktop--
Section Documentation: http://support.alertus.com/wiki/Alertus_Desktop

1. Install client on workstation for testing and evaluation IT
2. Choose client customizations *--AlertusDesktopAlert.exe.config file--*
   http://support.alertus.com/wiki/Customizing_Alertus_Desktop
   "About" text IT BO
   Alert System Label IT BO
3. Add Organizational logo (Logo1.gif file) IT BO
4. Determine client behavior *--AlertusDesktopAlert.exe.config file--*
   http://support.alertus.com/wiki/Desktop_Alert_Configuration_Options
5. Determine startup behavior IT
6. Determine system tray behavior IT
7. Alert Device Naming Convention IT
8. Specify polling interval IT BO
9. Test the Alertus Desktop Client by sending Alertus Activations IT BO
10. Disable Test Mode (AlertusDesktopAlert.exe.config file) IT
11. First draft of AlertusDesktopAlert.exe.config client configuration file for deployment testing IT
12. Deploying Alertus Desktop
    Section Documentation: http://support.alertus.com/wiki/Deploying_Alertus_Desktop
    a. Choose deployment method IT
    b. Deploy client to initial test group IT
    c. Review feedback from test group IT BO
    d. Final draft of AlertusDesktopAlert.exe.config file for organization wide deployment IT
    e. Compose and send notification to users of new alerting software. *--optional--* BO
       Deploy client across enterprise IT

EXHIBIT C
TECHNICAL REQUIREMENTS

A. Description of System

1. Software solution provided by Contractor shall include Alertus Server Software, Alertus Desktop Client and Alertus Console graphical user interface.
2. Overview of system ability:

    a. Alertus Desktop endpoints receive alerts and notifications within 1-2 seconds of activation.
    b. System shall allow or prohibit concurrent user sessions based on County-defined rules of behavior.
    c. Alertus Server software shall not limit the number of simultaneous users who can access the Alertus Console.
    d. Existing simultaneous use limitations shall not impact delivery of alerts or notifications to Alertus System endpoints
    e. No additional interfaces shall need to be purchased to work with Alertus System endpoints.
3. Contractor recommends County to have a physical or virtual server with Windows Server 2008 R2 32- or 64-bit, which can also run Windows Server 2003 and 2012 environments.
4. Contractor software solution shall be supported by Internet Explorer, Chrome, Mozilla Firefox and Safari
5. Scalability of Contractor software solution

    a. Alertus Desktop shall scale to tens of thousands to hundreds of thousands of recipients.
    b. Alertus Server Software and Alertus Console graphical user interface shall enable complete unified notification with all IT assets and facility infrastructure to enable a mass notification system, including:

        i. Digital signage override
        ii. Cable television override
        iii. Public address system control
        iv. Fire alarm monitoring and control
        v. Mobile application notification
        vi. Outcall or autodialing
        vii. VOIP phone notification
        viii. Two-radios integration
        ix. Panic button interaction
        x. Access control integration
        xi. HUGS/infant tracking system integration

    c. Contractor's software system shall be fully scalable regarding the number of users. Contractor recommends adding a new instance of Alertus Server to support each block of 60,000 users or end-points.
    d. Contractor shall support lateral scalability via Linked Alertus Servers to ensure all intended alert recipients receive notifications.
    e. Alertus Server shall be a unified solution and designed and installed as a single component. Contractor recommends to County to allocate Back-up Alertus Server to meet redundancy needs if the primary instances fail or becomes unavailable.

f. Contractor license shall be enterprise-wide for the Santa Clara Valley Health and Hospital, with an unlimited number of concurrent users.
g. Contractor software solution shall have its own embedded MySQL database and a MySQL driver shall be applied during installation.
h. Alertus Server license shall be generated specific to the scope of the design and shall not expire.
i. Contractor system shall protect the database records, which shall be accessed by multiple users, by implementing a shared and exclusive row level block in MySQL. Also, the application shall have layer locks to sensitive database methods and provide concurrency control, which the County may disable.
j. Contractor database shall be ACID compliant and shall implement transactions and access layer shall commit or rollback failed or incomplete transaction, as needed by the County.
k. Components required for the test system shall include:

    i. County provided and properly provisioned physical or virtual server
    ii. Alertus Server software
    iii. Alertus Desktop Client software
    iv. Any additional Alertus endpoints (i.e. Alert Beacons)

l. Contractor shall use MySQL InnoDB database, which has no hard limit on the number of records, as long as it remains within 2 TB- 64 TB.
m. Reporting tools shall be exported in the following formats:

    i. CSV format, which can be opened and modified in MS Excel
    ii. JfreeChart library, which can generate graphs or charts of the data

n. Contractor shall have two available application programming interfaces that can be used during testing with HHS, which shall enable integration with HIS:

    i. SOAP
    ii. REST

o. The minimum monitor resolution software solution shall support is 800 x 600, however, if a specific resolution is required, Contractor shall meet such requirements.
p. Change management process:

    i. Alertus Server update shall be prepared and available to the County through the MyAlertus portal.
    ii. County shall download and apply Alertus Server updates per instructions and in accordance with the County's change management procedures.
    iii. Contractor shall provide assistance through Alertus Support, as needed.
    iv. Alertus Server updates shall be notified to County via email and the MyAlertus portal, with confirmation by support representatives.

q. Generally available (GA) software versions
    i. The current generally available version of the Alertus Server Installer is 4.7.23, released on April 9, 2014.

ii. Contractor shall have two (2) significant GA releases annually. Contractor shall give the County, at minimum, three (3) weeks' notice of when these releases shall occur, which typically happen in August on January.
iii. Release updates shall be as required
iv. County shall be advised of releases or updates via email and through Alertus User Forum.
v. The Contractor's current software release is 1.14.4.2313. Full upgrades shall be tested and released every six (6) months. Email notifications shall be provided to the County.
vi. The County shall have complete control of moves, adds and changes, as well as scheduling software upgrades.

r. The response time from alert activation to the Alertus Desktop end-point receipt shall be no more than 2 seconds.
s. Customization of Contractor's software solution's system and graphical user interface:

i. User must have appropriate level of privilege to alter system and interface.
ii. User can alter
iii. Size
iv. Shape
v. Location
vi. Functionality
vii. Response options
viii. Visual appearance

t. Contractor's closest service representative is located in San Jose, CA.
u. Uptime/Downtime

i. Contractor's software system shall have uninterrupted availability.
ii. System uptime and planned downtime shall be dependent on County processes, infrastructure and needs.

B. Equipment and Software

1. Server hardware specifications:

a. Operating system: Windows Server 2008 R2 is recommended, but 2003 and 2012 are also supported.
b. Processors type and speed: Physical or virtual server with 4 GB RAM and a 3.0 GHz dual core CPU or better.
c. Redundancy: Separate physical or visual server meeting above specifications
d. System configuration: Minimum of 20 GB available hard desk space after provisioning
e. LAN connectivity: Gigabit recommended, but 10/100 shall be adequate for this size system.
f. Hard drive size: 200 GB minimum hard drive recommended

2. County must purchase the following hardware and software components:

a. Physical server or VM Ware
b. Microsoft OS

3. Contractor's software and agency components shall coexist with other software and applications on end-user devices by activating when user log-on to the end-device. Since the software resides in the Windows System Tray, which shall poll the Alertus Server for active applicable alerts. The software shall expand into a desktop notification requiring user interaction (i.e. acknowledgement) before the user can use other applications.

4. Contractor's system architecture shall be comprised of the following components:

   a. Altertus Console – which shall contain graphical user interface and shall operate in any web browser
   b. Alertus Server Software
   c. Alertus Desktop Client – which shall support all users

5. Contractor's software solution transaction processing capability shall process various transactions required by the County. The standard transaction shall be 1 kb with minimal bandwidth requirements.

6. Contractor's hardware support and escalation process shall be at the discretion of the County. The Contractor's Support Team shall provide support to numerous hardware environments and the County's complete system.

7. The County shall be responsible for the following required maintenance or support tasks, and any relevant maintenance schedule:

   a. Monitoring the Alertus Server software updates and apply accordingly
   b. Monitoring the Alertus Desktop Client software updates and apply accordingly.

8. Contractor's reporting software shall address the following topics:

   a. Alert History
   b. Device Acknowledgements
   c. Device activations
   d. Group memberships
   e. Device status
   f. CAP alerts

9. Contractor's reporting software shall export to Excel or Access.

C. Backup/Recovery

1. The Alertus Server shall be backed up at the County designated intervals using the Alertus Backup Utility.
2. Alertus Server shall automatically recover once power is reapplied.

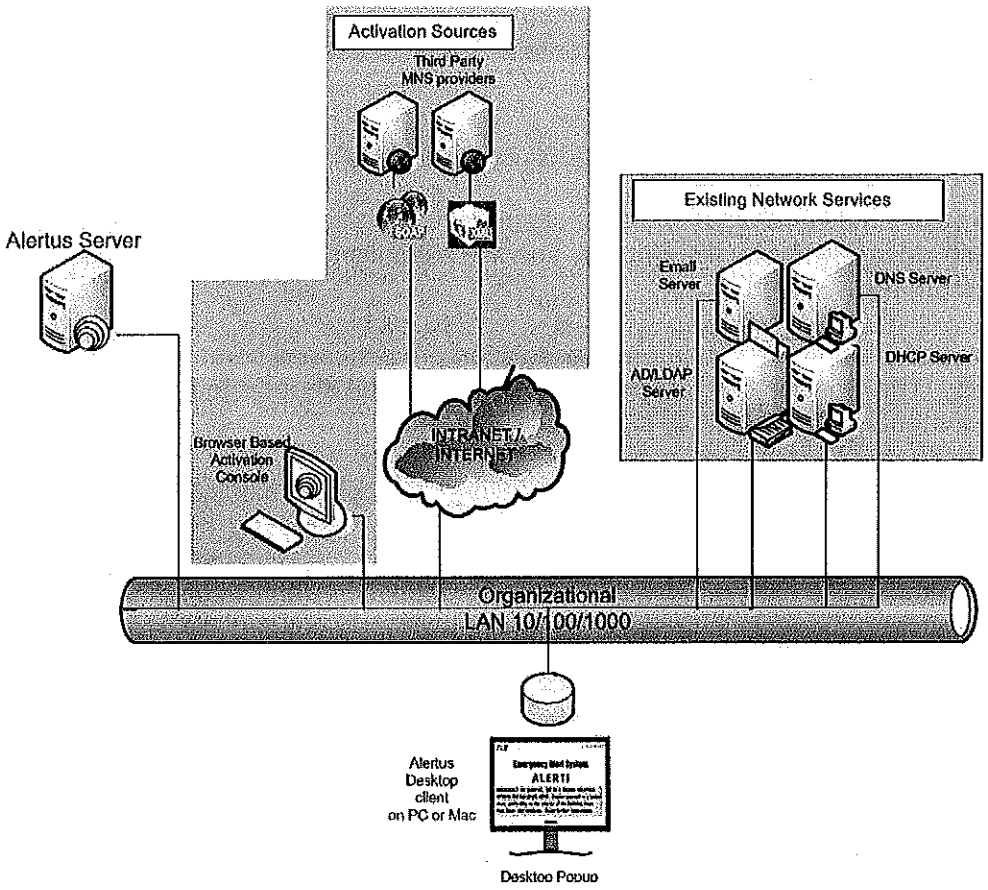
3. If Alertus Server hardware fails, Contractor shall take the necessary recovery steps, depending on failed component.

4. If the hard disk fails, Contractor shall have a backup image, which shall be applied.
5. Contractor assistance data shall be exported to a .CSV file at the request of the County.

D. Network/Hardware

1. Contractor shall not have any operational issues with the SCVHHS technical environment.
2. The following is the system/network design diagram:

Alertus System Architecture Overview



3. If County requires a virtual server, Contractor must use VM Ware 5.0.
4. No proprietary equipment shall be utilized.
5. There shall be no special networking requirements.
6. The response time shall be approximately 1-2 seconds from alert activation to receipt.

E. Storage

1. Contractor must retain data indefinitely. The County may back up data at predefined intervals.
2. Contractor shall store the data on non-proprietary media and in an industry standard format, which shall be used for short and long term storage.

3. The Contractor shall allow County configure data retention parameters within system settings. County shall leverage the Alertus Backup Utility, if needed.
4. Contractor shall utilize County database to store data records. The maximum amount of data the records are stored on shall depend on the available server hard disk size and hard disk expansion capabilities.
5. County shall print reports directly from Alertus Console to any network or local printers accessible to user.

F. Data Management

1. County data shall be exported and stored in the database in CSV file format. Contractor shall provide technical assistance to ensure database integrity is preserved.

G. Integration

1. Alertus Activation Console shall be web-based and the Alertus Desktop Client shall be installed on the County's endpoints.
2. Contractor's system shall be supported by IE7-IE10, all version of Mozilla Firefox, Chrome and Safari.
3. Contractor's system shall not require plug-ins to access and interact with Alertus Activation Console.
4. Contractor's SOAP API shall support consumption of alert relevant information, like CAP and NOAA feeds, which shall be used to activate Custom Event Triggers to activate County designated alerts.
5. Contractor's system shall not interconnect with the existing information system, since Contractor shall not process healthcare patient information.

H. Critical Updates, Patches and Antivirus

1. Contractor shall provide software updates reflecting any critical updates by Microsoft, etc. as needed.
2. Contractor shall use standard anti-virius software to protect data in real-time.
3. Contractor shall assist the County in fully correcting any emerging or discovered security vulnerabilities within 72 hours of notification from County or Contractor.
4. Cost of upgrades, including patches, corrections to defects, feature enhancements, minor and major version updates, shall be included in the first year. Subsequent years shall be covered as part of support, at no additional cost. Updates/patches provided in perpetuity shall be at no cost, regardless of support services.

I. Application Security Features

1. The Alertus Server shall support integration with LDAP version 2 or LDAP version 3 servers once the LDAP server is exposed to the Alertus Server. This integration shall be addressed during Alertus Server implementation.
2. Contractor's system shall be configured to authenticate users against an Active Directory tree with the Alertus Server, which shall supports this requirement through LDAP integration and single sign-on implementation.
3. Contractor's system shall log all log-in attempts and authenticate the level of privilege via the County database. County system administrators shall assign users to various existing and organization defined security.

4. Contractor's system shall allow the County to configure minimum password difficulty requirements and password lockout policies with the privileged system administrators through the System Configuration page of the Alertus Activation Console.
5. Contractor's system shall allow privileged system administrators to set password expiration policy, thereby requiring end-users to change their passwords at a specified interval through the System Configuration page of the Alertus Activation Console.
6. Contractor's system shall use port 443 HTTPS protocol to encrypt/decrypt transmitted information to authenticate users against an Active Directory tree.
7. Contractor's system shall establish user identity either with a user ID and password or a two-factor authentication, such as a smart-card and a PIN.
8. Contractor's system shall allow system administrators to create authorized user levels or use existing security roles. When the system administrators creates a user's account, they shall determine and select the level of privilege the user is granted. Security roles must be tailored to group designations.
9. The system administrators shall create new user accounts or security roles and level of privilege within the system configuration settings area of the Alertus Console.
10. Contractor's system must have a "user inactivity timeout" feature, which shall force a user to re-authenticate if idle for a preconfigured amount of time as determined by the County.

EXHIBIT D
FEATURES, FUNCTIONALITIES AND INTEGRATION REQUIREMENTS

Contractor guarantees that the installed software prior to final acceptance testing shall contain, at a minimum, the functionalities listed below If the solution does not contain the functionalities, the County reserves the right to un-install and return the software to Contractor and Contractor agrees to return all paid fees to the County.

A. Features and Functionalities

MANDATORY	
M001	Software solution shall have the capability to set up and modify notification groups
M002	Pop-up Notifications on workstations by predefined groups
EMERGENCY NOTIFICATION	
EN01	Ability to perform functions with minimal keystrokes
EN02	Graphical interface for ease of use
EN03	Ability to quickly and easily distribute alerts and messages
EN04	Ability to customize alerts and messages
EN05	Real-time graphical status feedback from notified users
EN06	Multiple ways of initiating events
EN07	Provide help via function key or icon from any screen or field
EN08	Ability for administrator to edit/add to on-line help text. Contractor shall maintain an active Wiki site to support user help additions until incorporated into the solution build by Contractor. Contractor shall offer any additional help text options at no additional fee.
EN09	Ability to use upper and lower case letters
EN10	Additional notification methods (cell phone messages, e-mail, etc.)
EN11	Provide 24x7 hour system availability
EN12	The system should allow the database to be backed up without interrupting operations or performance
	System should provide:
EN13	a. On-line context-sensitive help functions
EN14	b. On-line user-friendly tutorial
EN15	c. Site-specific on-line documentation and user guide

EN16	d. System Manager's Guide - An on-line version of this documentation is desired to allow key word searching to facilitate location of the needed text. Contractor shall also have a System Administrator's Guide.
EN17	Contractor support shall be available 24 hours a day 7 days per week.
EN18	Support via remote capability
EN19	If a workstation fails, its replacement should be easily added to the notification system
EN20	System notification response time must be timely (less than 2 seconds on the LAN and less than 3 seconds at remote or wireless terminals).
EN21	Ability to set up mobile command centers, as well as support decentralized execution or alert origination.
EN22	Ability to import from existing solution (REACT) of notification screens and group designations
EN23	The capability to utilize an available satellite system for remote locations in the event normal network connectivity is down. Contractor shall support a warm failover to an alternative location.
SECURITY	
S001	Maintain the following user security information and audit trail: a. User ID b. User name c. Notifications sent and updates or deletions made d. Group or user notification sent to
S002	Automatically log out user after 15 minutes of inactivity, with no loss of data, except for unsaved templates under development.
REPORT WRITING	
R0001	Ability to selectively edit information
	Ability to selectively print information:
R0002	Print single screen or message
R0003	Print a group or all records
R0004	Print audit and notification history
R0005	Print all messages and screens
R0006	Ability to send reports to screen (on-line viewing)
R0007	Ability to e-mail report
R0008	Ability to print agency logos on reports

R0009	Ability to print management summary reports:
R0010	Ability to schedule and automatically generate daily, weekly, monthly, annually, and "user defined date range" reports based upon the pre-determined schedule, and also based upon request
	System should provide:
R0011	On-line context-sensitive help functions
R0012	On-line user-friendly tutorial
R0013	Site-specific on-line documentation and user guide
R0014	System Manager's Guide - An on-line version of this documentation is desired to allow key word searching to facilitate location of the needed text.
R0015	Vendor support available 24 hours a day 7 days per week

B. INTEGRATION REQUIREMENTS

1. Contractor shall have several methods of interoperability, including push, pull, and query.
2. Contractor shall have an open API; supports CAP, RSS, and several other standard connection methods.
3. Contractor shall not charge any additional fees for integration connections.
4. Contractor's system shall integrate with Peoplesoft and other systems using SOAP or REST APIs.

EXHIBIT E
SERVICE AND SUPPORT REQUIREMENTS

1. On-Going Service and Support

a. Post Implementation Follow Up

i. Contractor technical support personnel shall assist post live-system debugging and bringing application into full conformance as specified under Exhibit C - Technical Requirements and Exhibit D – Features, Functionalities and Integration.
ii. Contractor shall check in every six months to review performance of solutions utilized.
iii. System documentation (electronic) shall be provided via email and via access to the Alertus customer supported Wiki website. Future updates and releases shall be emailed directly to the County's point of contact.
iv. The County shall have complete control of moves, adds and changes, as well as scheduling software upgrades.

2. Training Plan

a. Training for Power users/administrators, general users, Content creators and Instructors:

Alertus Activation / Dispatch Manager Training - This training shall include:

i. Review of the purpose of Alertus;
ii. All sending features including single user, groups, locations, device types;
iii. Group creation and management;
iv. User creation;
v. Delegation of sending and management privileges;
vi. Initial troubleshooting of devices;
vii. Discussion on other configurations possible with Alertus; and
viii. A general question and answer session.

b. Training for Technical administrators:

Alertus System Administrator Training - The system administrator training is for Alertus administrators who shall be authorized to make system-wide changes to the Alertus Server. This training shall include:

i. Changing of device configurations;
ii. Creation/editing of alert groups and locations;
iii. Custom Event Triggers;
iv. Enabling/disabling send options, Integration via CAP or Alertus API;
v. Editing and maintaining Alertus Middleware options;
vi. Alertus Threatwatcher settings and logic;
vii. Device Assignment Rules and logic; and
viii. Other topics as required.

c. Training of technical operation staff and support staff:

Alertus Technical Overview Training - This lecture and discussion training shall

provide a technical overview of the Alertus system installed and shall include:

i. Basic functionality,
ii. Network traffic,
iii. IT dependencies
iv. Delineate the needs for and effect of having the Alertus server plugged in to the IT infrastructure
v. Aid with support and/or future IT changes to maintain Alertus functionality.

Note: Per groups outlined above, training is typically coordinated by group and provided via a webinar (through Go2Meeting, WebEx or Join.me conference services) or onsite.

d. Training shall be provided on-site or via an interactive Webcast and Alertus Customer Support Portal website.
e. The recommended training curriculum shall include system overview and coordinate a training schedule, which shall include webinar training to review the Alertus Activation Software.
f. The number training sessions shall be mutually agreed upon, as well as the dates and times.

Any and all training shall take place after the Alertus Activation software is installed, administered and accessible by all that require training. Follow-up training shall be available throughout the first year and continues to be available under continued subscription to the Enhanced Notification Services.

EXHIBIT F
COUNTY OF SANTA CLARA STANDARD TERMS AND CONDITIONS
FOR AGREEMENT FOR INFORMATION TECHNOLOGY GOODS AND RELATED SERVICES

This Agreement is entered into and is effective November 26, 2014, between the County of Santa Clara, (hereafter referred to as "County") and Alertus Technologies, LLC (hereafter referred to as "Contractor"), to provide an emergency management notification software system (hereafter referred to as "Emergency Management") with Contractor including all related services and maintenance. It is mutually agreed between the parties:

1. Agreement 5500002508

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 November 20, 2014.

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 Exhibits), 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 exhibits 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 Exhibit A of this Agreement is the basis for the pricing and compensation plan. The maximum compensation paid to the Contractor under this Agreement is $59,750.

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 Exhibit 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 exhibit 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 Exhibit F.

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 Exhibit F 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.

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 exhibits exist, the terms and conditions in this Agreement shall control over its exhibits.

58. ENTIRE AGREEMENT

This Agreement and its exhibits (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: Jennifer Ngo
Contract Administrator
c/o Procurement Department
2310 North First Street, Suite 201
San Jose, CA 95131-1040

CONTRACTOR:
Name: Ryan Ockuly

Title: National Sales Director

Company: Alertus Technologies, LLC

Address 1: 11785 Beltsville Road

Address 2: 15th Floor

City: Beltsville

State: MD

Zip: 20705

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, exhibit, 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.

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. BEVERAGE NUTRITIONAL

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.

67. 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.

68. 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.

EXHIBIT G
ALERTUS LICENSE AND SUPPORT AGREEMENT

This License and Support Agreement (**"Agreement"**) is made this November 26 day of 2014, (the **"Effective Date"**) between Alertus Technologies, LLC, a Maryland corporation (**"Alertus Technologies"**), located at 11785 Beltsville Drive, Suite 1500, Beltsville, Maryland 20705, and the Santa Clara Valley Health and Hospital System ("SCVHHS / **Licensee**"), located at .

1 **Definitions.**

1.1 **"Documentation"** means written and/or on-line material provided by Alertus Technologies to assist Licensee in the use of the System.

1.2 **"Effective Date"** means the date set forth above.

1.3 **"Equipment"** means the Equipment or comparable equipment delivered by Alertus Technologies hereunder.

1.4 **"Site"** means Licensee's location at .

1.5 **"Software"** means the Alertus Technologies software programs and any updates, modifications and corrections thereto provided by Alertus Technologies to Licensee hereunder.

1.6 **"Third Party Software"** means any software developed by a third party which is installed by Alertus Technologies on the Equipment.

1.7 **"Initial Support Term"** means the period beginning the day after the Parties determine implementation of the Equipment and Software are complete and ending one (1) year after such date.

1.8 **"Initial Warranty Period"** means the period beginning the day after the Parties determine implementation of the Equipment and Software are complete and ending one (1) year after such date.

2 **Delivery of Software and Equipment.** Licensee shall properly prepare to accept delivery of the Equipment and Alertus Technologies shall deliver the Equipment to Licensee. In no event shall Alertus Technologies be responsible for delays in delivery or installation or any damages to Licensee resulting from any delay. Title and risk of loss shall pass to Licensee upon shipment.

3 **Installation and Training; Licensee Data; and Technical Support Level.**

3.1 **Installation.** Alertus Technologies shall provide installation as set forth in **Exhibit A – Payment Terms.**

3.2 **Training.** If purchased by Licensee, the nature and duration of training services shall be reflected on **Exhibit A – Payment Terms**. The term of any annual training subscription purchased by Licensee shall expire with the Initial Support Term.

3.3 **Licensee Data.** Licensee shall have responsibility for the accuracy or functionality of any data it places into the Alertus System ("Licensee Data") and for adherence to any privacy act or regulation regarding such Licensee Data it selects and stores onto the Alertus System. Licensee also shall be solely responsible for communicating any applicable notices or terms of use to its registrants. These duties and obligations are non-delegable by Licensee to Alertus Technologies.

4 **Technical Support Level of Service.** If purchased by Licensee, the nature and duration of technical support services shall be reflected on Exhibit A. Technical Support shall be Enhanced Notification Service & Support – Gold.

5 **Software Support Services.**

5.1 Subject to the terms of this Agreement and provided that Licensee pays the fees specified in this Section 6.1, Alertus Technologies shall provide Licensee with the support services described in **Schedule A**, the Alertus Technologies Technical Support Center Services Plan. Licensee shall provide Alertus Technologies with all information, documentation, technical assistance, and access to the Site as Alertus Technologies may require in order to provide services hereunder.

6 **License Grant.**

6.1 **Scope.** Alertus Technologies hereby grants to Licensee, and Licensee accepts, a non-exclusive, non-transferable license to use the object code version of the Software and the Documentation for its internal business purposes, including public services, at the Site in accordance with this Agreement. Licensee may use the Software only on the Equipment or substitute equipment approved in writing by Alertus Technologies. Licensee may make one copy of the Software for backup purposes only but shall include therein all proprietary marks and notices included in the original. Licensee may not otherwise copy or permit the copying of any part of the Software or Documentation.

6.2 **Restrictions on Use.** Licensee may not, directly or indirectly, (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Software; (ii) modify, translate, or create derivative works based on the Software; (iii) copy (except for archival purposes), rent, lease, resell, sublicense, distribute, assign, or otherwise transfer rights to the Software, except as otherwise provided herein; (iv) use or allow the transfer, transmission, export, or re-export of the Software in violation of any export control laws or regulations administered by the U.S. Commerce Department, OFAC, or any other government agency; or (v) remove any proprietary notices or labels on the Software.

6.3 **Updates and Upgrades.** Updated or upgraded versions of the Software may be created or issued by Alertus Technologies from time to time. If the Software is an updated or upgraded, Licensee is bound by the terms of this License and may only use that updated or upgraded Software in accordance with this License. Alertus Technologies may, at its sole discretion, require the installation of software updates or upgrades to maintain any applicable warranty.

6.4 **Intellectual Property, Trademark and Copyright.** Alertus Technologies retains ownership of the Software, any portions or copies thereof, and all rights therein. Alertus Technologies reserves all rights not expressly granted to Licensee. This License does not grant Licensee any rights in connection with any trademarks or service marks of Alertus Technologies, its suppliers or licensors. All right, title, interest and copyrights in and to the Software and the accompanying Documentation and any copies of the Software are owned by Alertus Technologies, its suppliers or licensors. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This License grants Licensee no rights to use such content.

6.5 **U.S. Government Restricted Rights.** The Software and associated Equipment and Documentation are provided with RESTRICTED RIGHTS. With respect to any acquisition of the Software by or for any unit or agency of the United States Government ("Government"), the Software shall be classified as "commercial computer software," as that term is defined in the applicable provisions of the Federal Acquisition Regulation ("FAR") and supplements thereto, including the Department of Defense (DoD) FAR Supplement ("DFARS"). The Software was developed entirely at private expense and no part of the Software was first produced in the performance of a Government contract. If the Software is supplied for use by DoD, the Software is delivered subject to the terms of this LICENSE and either (i) in accordance with DFARS 227.7202-1(a) and 227.7202-3(a) or (ii) with restricted rights in accordance with DFARS 252-227-7013 (Oct. 1988), as applicable. If the Software is supplied for use by Government agency other than DoD, the Software is restricted computer software delivered subject to the terms of this LICENSE and (i) FAR 12.212; (ii) FAR 52.227-19; or (iii) FAR 52.227-14, as applicable.

7. **Infringement Indemnity.** With the exception of any third party software, hardware or equipment that may be provided under this Agreement, Alertus Technologies agrees to hold Licensee harmless from liability to third parties resulting from infringement of any United States patent or copyright or trade secret by the Alertus Technologies software purchased hereunder and Alertus Technologies further agrees to pay all damages and costs, including reasonable legal fees, which may be assessed against Licensee under any such claim or action. Alertus Technologies shall be released from the foregoing obligation unless Licensee provides Alertus Technologies with (i) written notice within forty-five (45) days of the date Licensee first becomes aware of such a claim or action, or possibility thereof; (ii) sole control and authority over the defense or settlement thereof; and (iii) proper and full information and assistance to settle and/or defend any such claim or action. Without limiting the foregoing, if a final injunction is, or Alertus Technologies believes, in its sole discretion, is likely to be, entered prohibiting the use of the software by Licensee as contemplated herein, Alertus Technologies shall, at its sole option and expense, either (a) procure for Licensee the right to use the infringing software as provided herein or (b) replace the infringing software with noninfringing, functionally equivalent products, or (c) suitably modify the infringing software so that it is not infringing; or (d) in the event (a), (b) and (c) are not commercially reasonable, terminate the license, accept return of the infringing software and refund to Licensee an equitable portion of the license fee paid therefor. Except as specified above, Alertus Technologies shall not be liable for any costs or expenses incurred without its prior written authorization. Notwithstanding the foregoing, Alertus Technologies assumes no liability for infringement claims with respect to software (i) not supplied by Alertus Technologies, (ii) made in whole or in part in accordance to Licensee's specifications, (iii) that is modified after delivery by Alertus Technologies, (iv) combined with other products, processes or materials where the alleged infringement relates to such combination, (v) where Licensee continues allegedly infringing activity after being notified thereof or after being informed of modifications that would have avoided the alleged infringement, or (vi) where Licensee's use of the software is not strictly in accordance with this Agreement. **THE FOREGOING PROVISIONS OF THIS SECTION STATE THE ENTIRE LIABILITY AND OBLIGATIONS OF ALERTUS TECHNOLOGIES AND THE EXCLUSIVE REMEDY OF LICENSEE WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADE SECRET, TRADEMARK OR OTHER INTELLECTUAL PROPERTY RIGHT BY THE SOFTWARE.**

8. **Injunctive Relief.** Each party acknowledges that a violation or threatened violation by it of Section 9 or 10 hereof would result in damage that is largely intangible but nonetheless real and that is incapable of complete remedy by award of damages. Thus, such violation or threatened violation shall give the injured party the right to a court-ordered injunction to specifically enforce such covenant or obligation. The party in violation of any such section shall pay as damages reasonable expenses, including but not limited to attorney fees, incurred in obtaining specific enforcement.

9. **Partial Invalidity**. If any provision of this Agreement is ruled wholly or partly invalid or unenforceable by a court or other government body of competent jurisdiction, the validity and enforceability of all provisions of this Agreement not ruled to be invalid or unenforceable shall be unaffected.

10. **Third Party Beneficiaries**. None of the provisions of this Agreement is intended by the parties, nor shall they be deemed, to confer any benefit on any person not a party to this Agreement.

Alertus Technologies

By: _____

Title: CEO

Date: 11/25/2014

Licensee

By: _____

Title: _____

Date: _____

SCHEDULE A

Technical Support Center - Support Plan for On Premise Systems

Alertus Technologies ("Alertus Technologies") offers Alertus Technologies Software and Hardware support to purchasers ("Licensee" or "Customer") of its application Software and Hardware, in accordance with the terms and conditions of this Technical Support Center Services Plan ("Support Plan"), which is made a part of and incorporated by reference into the License and Support Agreement entered into by Customer and Alertus Technologies. Defined terms as set forth in the License and Support Agreement shall have the same meaning in this Support Plan. This Support Plan does not apply to system software or hardware, or any other third party software.

Conditions of the Support Plan

In order to keep the Support Plan active, the Customer is required to: Pay all applicable Customer Support Plan Fees (i.e. Gold plan); and Comply with all terms and conditions of this Support Plan and the License and Support Agreement.

Definitions

Response Time is the period of time that it takes the Technical Support Center ("TSC") to call the Customer back after: 1) the Customer has left a voice mail; 2) an email addressed to the TSC group distribution email address is received; or 3) the Customer has submitted a support ticket through the Alertus Customer Portal, or provide an update on the support ticket. Response times are only implemented when the call is not resolved on the first call. Response Time does not mean Resolution Time.

Resolution Time is the period of time it takes to solve a problem. The resolution time is different for each situation and cannot be determined until the appropriate TSC personnel have evaluated the problem and is able to determine an approximate resolution time.

TSC	Technical Support Center
TSS	Technical Support Specialist
TSA	Technical Support Analyst

Technical Support Levels

Alertus Technologies shall offer the Enhanced Notification Service and Support – Gold Annual Support package

The County shall receive all service and support listed under Silver and Gold.
The following summarizes the services available to Customers under the Gold support level during the period covered by the Support Plan

ENHANCED NOTIFICATION SERVICE & SUPPORT – SILVER

- Technical Support Center: Unlimited Email and Live Phone Support during normal weekday business hours (8AM – 5PM ET, Monday – Friday)
- Software Updates: Critical bug fixes (i.e. patches), upgrades, and prioritized feature requests
- Training and Documentation: Documentation Portal access, two System Administrator and two System User training webinars, and unlimited training video access

- Application Programming Interface (API) and Integration Support: Third Party SOAP API access with integration / Developer support
- Monitoring: Passive device status web page monitoring, and real-time device status notifications. On-site Alertus device inspection and professional services at a discounted rate
- Advanced Services: GIS Mapping, ThreatWatcher, opportunity to Pilot Beta products and new functionality, and monthly Security Patch Installation Notices (SPIN) detailing Alertus and third-party security patch applicability and installation instructions

ENHANCED NOTIFICATION SERVICE & SUPPORT – GOLD

- All the benefits listed under the Enhanced Notification Service & Support - Silver Plan above
- Technical Support Center: Unlimited Email and Live Phone Support during normal weekday hours, plus Emergency Phone Support 24/7
- Comprehensive Hardware Warranty: Hardware warranty addresses only Alertus devices and hardware and includes firmware updates for Alertus devices. Annual Warranty service includes:

  ✓ Troubleshooting and repair in Alertus Technologies offices located in Beltsville, MD
  ✓ Replacement of defective hardware with hardware of same model/version
  ✓ Newer model/version hardware replacement at prorated cost to Client is optional in instances where same model/version hardware is not available or unacceptable
  ✓ Shipping and Handling costs to return hardware to Client location

- Annual hardware support **does not** include:
  ✓ On-site troubleshooting or repair
  ✓ Client shipping costs to return hardware to Alertus Technologies for servicing
  ✓ On-site installation of serviced hardware
  ✓ Servers, switches, wireless access points and other network hardware are not automatically covered under Premier plus Warranty, but may be added at Client request for an additional fee

Support Services Provided

Supported Products

The TSC shall only support Software and Hardware approved by Alertus Technologies. The TSC shall not resolve requests associated with software other than that provided by Alertus Technologies; the requests shall, however, be logged into the database. Third Party Software loaded by Customer on an Alertus Technologies system without Alertus Technologies' prior written approval voids the associated Software Warranty and this Support Plan. Pursuant to this Support Plan, Alertus Technologies, as coordinated by its Technical Support Center, shall provide issue resolution and updates to supported Software as further described below.

Hours of Operation

Normal Business Hours (NBH): Monday through Friday, excluding County holidays, from 8:00AM to 5:00PM, Pacific Time.

After hours Emergency support only - see Technical Support Levels and Call Levels

Services Provided

Issue Resolution
The TSC works with Customers to resolve issues related to supported Software and Hardware that does not perform materially in accordance with the current Documentation for such Software and Hardware. This service is designed to support the Customer's technician who is adequately trained in the Alertus product about which they are calling and listed as an approved Customer Contact with Alertus Technologies' TSC. To be adequately trained the Customer's technician must have received training directly through an Alertus Technologies training program or have been trained by a Customer Technician that has received training directly through Alertus Technologies. A trained Customer's technician is responsible for attempting to troubleshoot issues prior to calling TSC. If the Customer's technician is not adequately trained, based on the description above, in the product about which he or she is calling, and thus not listed as an approved Customer Contact, Alertus Technologies TSC personnel shall attempt to contact an approved Customer contact for problem resolution.

For security purposes, only Customer contacts that are listed with TSC shall receive support unless a listed contact provides approval to do so. In the event of an emergency TSC may make a special allowance if TSC personnel are unable to reach one of the listed contacts for verification.

To better facilitate high first call resolution, the TSC shall utilize remote access software if acceptable to the Customer. This shall allow the TSC to connect to the Customer's system via a remote connection and actively control the system to perform troubleshooting and/or resolution services. The TSS/TSA shall at all times advise the Customer of their intention to access the system, and upon completion shall advise the Customer that they have left the system, relaying to them what steps were taken to resolve an issue.

The TSC shall maintain a database of all calls received from the Customer, the steps taken to resolve the problem and the final resolution. The database shall show dates when a call was received and dates of all contacts related to call.

TSC shall work with the Customer to identify errors or defects in the Software or Hardware, and if the TSC is unable to confirm that such error or defect exists through independent testing, it shall then escalate the issue to Alertus Technologies' R&D Department. The TSC shall remain as the Customer contact and shall work with the R&D Department to provide updated information to the Customer through resolution of the issue.

Hardware Support
Alertus Technologies' TSC shall track hardware issues related to the system during the Initial Support Period and, if a hardware warranty is purchased through Alertus Technologies from third party vendors, Alertus Technologies shall contact the appropriate vendor for warranty repairs. For subsequent years the Customer has the option to extend their warranty by contacting Alertus Technologies Sales. The Alertus Technologies TSC shall continue to work with the Customer to diagnose and make recommendations on hardware issues.

Contacting the Alertus Technologies Technical Support Center

During Normal Business Hours: Customers may call TSC at 866.425.3788, Extension 2. If all TSC personnel are busy assisting other customers, the call shall go to voice mail. If the caller is experiencing an emergency (see Call Levels below) they may hit 00 for the operator and a TSC manager shall be paged to assist.

If the call is not an emergency (as defined below), the caller should leave a message with their name, company name and ID, telephone number and a brief description of the reason for the call. Messages are checked frequently and calls are returned in the order in which they are received, but normally within two (2) hours.

Customers may also request assistance by emailing the TSC at Support@Alertus.com, or by logging into the Alertus Customer Portal and submitting a new support ticket.

After Hours Emergency: If the Customer is experiencing an emergency (as defined below) and has subscribed to Enhanced Notification Service & Support at the Gold or Platinum level, they should call the TSC at 866.425.3788, Extension 811 or 911. The call shall be routed to an answering service where the Customer should leave a clear message with their name, organization name, telephone number and a brief description of the reason for the call. The on-call TSS shall be paged and shall return the call within 15-minutes of receipt of the page.

***Email Requests*:** The TSC shall respond to e-mail requests within eight (8) business hours. **Note:** Emergency or very important requests should always be phoned into the TSC. E-mail can sometimes be unreliable and the TSC has no control over the timely delivery of requests. E-mail service level commitments are based on the time the requests actually reach the TSC. The email address for the TSC is Support@Alertus.com.

Call Levels applied to this Support Plan

Emergency Call - Immediate Response during NBH regardless of Enhanced Notification Service & Support level; within 15-minutes of page outside NBH for Enhanced Notification Service & Support Gold or Platinum subscribers

- Alertus Server shall not boot or complete Alertus hardware failure.*
- Server Applications shall not start.
- Site is experiencing an actual emergency and the system shall not send out notifications to one or more device types.
- Site initiates activation, attempts to stop it, and experiences difficulty doing so.

*If it is determined the system failure is due to software or hardware loaded without coordination with Alertus Technologies or other acts induced by the end user, resources shall be allocated as available to assist but response time is not guaranteed.

Routine Call – 2-hour Response Time

- Attempting to perform maintenance and needs assistance.
- Experiencing partial hardware failure or needs to troubleshoot possible hardware problems.
- Reports are not functioning properly.
- Testing system and needs help making adjustments.
- Assistance with modifying Alertus System Settings or groups.
- Assistance with Threat Watcher or other alert feeds.
- Assistance creating template scenarios.

Services that require advanced scheduling

- Installation of software or hardware updates or addition.
- Modifications to the system to accommodate Alertus device changes.
- Alertus Technologies and third-party solution integration issues.
- Map interface issues.

Call Procedures & Escalation

The Technical Support Center shall maintain call ownership throughout the entire request process. The TSC shall address incoming calls as follows.

1. Capture the Request - The TSS/TSA shall capture all requests by phone, e-mail, Alertus Customer Portal, or voice mail and verify the right to service based on the Customer's name, support contract status and the approved license profile. If the request relates to unsupported software or Alertus functionality for which the Customer is not licensed, the Customer shall be notified. Otherwise, the analyst shall continue with Step 2.
2. Log Request into the Database - The TSS/TSA shall open a ticket in the Support Portal. Information included on the ticket shall include the Customer's name, location, description of problem, severity of problem, and time of request and person reporting the issue.
3. Troubleshoot the Request –

    a. The TSS/TSA responsible for resolving the call shall acknowledge the open ticket and work with the Customer to resolve the issue.
    b. When issue is identified and troubleshot, short-term remedies shall be identified, when appropriate.
    c. Corrective actions or possible corrective actions shall be identified and escalated to management for approval and resource allocation and required tasks shall be completed.
    d. Resolution shall be applied and tested in non-production environment
    e. Version updates shall be packaged and released.
    f. County shall be notified of resolution and when the update shall be available.
    g. County shall download and apply the update.

4. Escalate to Second Level - The TSS shall escalate the request to second level support when the first contact is unable to make progress in the resolution of the issue in a timely manner.
5. Log Resolution into the Database - The TSS/TSA shall log the resolutions to requests in the Support Portal.
6. Verify Customer Satisfaction - The TSS/TSA shall follow up and verify that the Customer is satisfied with the resolution.
7. Close the Request or Ticket - All tickets shall be closed after the Customer satisfaction has been verified.

Customer Responsibilities

- Hardware Operating Environment. It is the Customer's responsibility to ensure that the hardware-operating environment is fully functional and meets Alertus Technologies' minimum operating requirements for the Alertus Technologies Software supported hereunder.
- Operating System and Ancillary Software Environment. It is the Customer's responsibility to ensure that the operating system and ancillary software are fully functional, commercially available (except as otherwise agreed to in writing by Alertus Technologies) and meet Alertus Technologies' minimum operating requirements for Alertus Technologies' Software product(s).
- The Customer shall maintain an Alertus Technologies application software release that is the most current version of the Software or one version back from the most currently released version.
- The Customer Site should have at least one system administrator that has attended Alertus Technologies training. The Customer shall provide the administrator's contact information to Alertus Technologies.

- The customer shall perform regular maintenance to keep the system in optimal condition. This includes performing regular backups and creating emergency repair discs when changes are made, de-fragmenting the hard drive on a regular basis, and testing the system at regular intervals.
- Customer shall schedule install of all updates in a timely manner.
- Customer shall work with TSC staff to maintain an accurate database of contact names.
- Customer shall respond to requests for information in a timely manner.
- The Customer shall not add software to the system without prior Alertus Technologies approval.
- Customer shall not move the system to a new location without notifying Alertus Technologies.
- Payment of all support fees when due. Failure to renew support fees before the expiration of the then in effect support term shall result in the imposition of a reinstatement fee at Alertus Technologies' then current rate before resumption of support services.

Support Limitations

Alertus Technologies' support obligations hereunder shall not apply to any Alertus Technologies supported application Software or Hardware if correction of an error, adjustment, repair, or parts replacement is required because of:

- Accident, neglect, tampering, misuse, improper / insufficient grounding, failure of electric power, failure of the end user and/or others to provide appropriate environmental conditions, relocation of hardware or software, or causes other than ordinary use.
- Repair or alteration, or attempted repair or alteration of any Alertus Technologies supported product (hardware and/or software) by the end user or others and not by Alertus Technologies.
- Damage or destruction caused by natural or man-made acts or disasters.
- Failure or degradation in performance of Alertus Technologies supported equipment (hardware and/or software) due to the installation of another machine, device, application or interface not specifically certified and approved by Alertus Technologies for use.
- The operation of the software in a manner other than that currently specified by Alertus Technologies.
- The failure of the Customer to provide suitable qualified and adequately trained operating and maintenance staff.
- Incompatible or faulty Customer equipment.
- Modifications made without Alertus Technologies' written approval to the OS, network, hardware or software environment or software applications.

Further, support described herein does not include cosmetic repairs, refurbishment, furnishing consumables, supplies or accessories, making accessory changes or adding additional devices or software applications.

Telephone support and/or field engineering to rectify such unsupported failures as described above may be obtained from Alertus Technologies on a time & materials basis as set forth in the applicable price list. The labor rate charged shall be the then current Alertus Technologies labor rate (plus expenses) at the time service is requested.

Software Updates

Alertus Technologies shall provide application Software updates. Application Software updates are defined as minor enhancements to the already purchased product feature / functionality set. A product change is classified as minor, in the discretion of Alertus Technologies, based upon the impact of the change to the core functionality of the product. Notice of all Software updates available during the term of the Support Plan shall be posted under "latest release notes" for each product (e.g. Alertus Sever, Alertus Middleware, Alertus Desktop, etc.) on the Alertus Technologies Support

Website located at https://helpdesk.alertus.com/support (login required). Application Software program updates shall roll into the existing Support Plan, thereby not extending the term of the Support Plan.

Other Services

Other services not specifically identified as being included in this Support Plan, including but not limited to training, implementation services, and custom development, are not included.

EXHIBIT H
INSURANCE REQUIREMENTS
Professional Services Contracts
(e.g. Medical, Legal, Financial services, etc.)

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

EXHIBIT H
INSURANCE REQUIREMENTS

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. Products/Completed Operations aggregate - $1,000,000

   d. Personal Injury - $1,000,000

2. General liability coverage shall include:

   a. Premises and Operations

   b. Personal Injury liability

   c. Products/Completed

   d. 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 Contractor'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:

2. 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.

3. 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. Contractor's obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.

4. 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.

5. 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.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

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.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

6. Person Authorized to Act on Behalf of Parties

The following persons are the designees for purposes of this Agreement:

Contractor: Title/ Designee Ryan Ockuly, National Sales Director

County: Title/ Designee _____

Either party may change the aforementioned names and or designees by providing the other party with no less than three (3) business days 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).

2. VPN Site-to-Site ☐ Primary ☐ Backup ☐ N/A

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

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:

b. 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.
c. The PIN number is confidential, County-owned, and will be identified as such.
d. 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.
e. 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.
f. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.
g. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.
h. 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.
i. The PIN number will be issued to Contractor following execution of this Agreement.
j. 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 Model ☐ 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:

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

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.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS
Signatures of Contractor Employees receiving CryptoCards (if issued by County):

CONTRACTOR: N/A

Type Name: _____

Title: _____

Date: _____

CONTRACTOR: _____

Type Name: _____

Title: _____

Date: _____

CONTRACTOR: _____

Type Name: _____

Title: _____

Date: _____

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS
September 2010

SANTA CLARA COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT INSTRUCTIONS

In May 1995 the Board of Supervisors charged each County organization with the responsibility for ensuring that all County employees had read and signed a statement of responsibility concerning use of the County's networks and information systems. The resulting County-wide User Responsibility Statement is intended as a *minimum* statement of User responsibility, and individual County Agencies and Departments may require Users to read and sign additional statements to meet any special requirements that apply within their own environments.

- The County User Responsibility Statement must be signed by anyone who might reasonably require access to a County network and/or information system. This includes all County employees, as well as any other individual who needs authorized access for County business purposes. All Users who are allowed to access County resources remotely must also sign an additional attachment specifically related to remote access; this is included as Attachment A of the User Responsibility Statement. In addition, Users who are granted approval to use a personally-owned device for County business must also sign Attachment B of the User Responsibility Statement.
- By signing the Statement or its attachments, Users acknowledge that they have read and understand the contents and that violation of any of the provisions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.
- If an individual refuses to sign the Statement, the Department can choose to read the Statement to the individual, who will be required to verbally acknowledge understanding of the Statement's contents in the presence of two or more responsible managers. These managers will attest in writing that this reading and verbal attestation of understanding occurred. Failing this verbal acknowledgement of understanding, the involve individual will be denied access to all County information systems and networks.
  - Each County organization is responsible for storing and maintaining the signed Statements of its own Users.
- All County organizations shall have their Users re-execute the Statement and/or attachments annually, or whenever there is an update or other change to the Statement or attachments (Department Heads will be notified by the County CIO's office of any updates or changes to the Statement or attachments).
- Each County organization should identify a "User Responsibility Statement Administrator." This is an occasional personnel function that should NOT be filled by

other individual who has been authorized to access County networks and systems.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

1. General Code of Responsibility

Key Points

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 minimum 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. If a User is unclear as to the appropriate standards, it is that User's responsibility to ask for guidance from appropriate information systems support staff or Department management.

You are responsible for your own behavior.

If you're unclear about a security standard, it's your responsibility to ask for guidance.

1.2 Users must comply with basic County standards for password definition, use, and management.

You must comply with County password standards.

1.3 With the exception of County-owned and approved devices issued to specific authorized County users, only authorized information systems support staff may attach any form of computer equipment to a County network or system unless express written permission to do so is given by Department management. This includes, but is not limited to, attachment of such devices as laptops, PDAs, peripherals (e.g., external hard drives, printers), and USB storage media.

Don't attach computer equipment of any kind to County systems or networks without permission.

1.4 The use of personally-owned USB storage media on any County computer system is prohibited. All such devices must be County-owned, formally issued to the User by the Department, and used only for legitimate County business purposes.

Use only County-owned and issued USB storage media.

1.5 Connecting County owned computing equipment, including USB storage media, to non-County systems or networks is prohibited unless express written permission has been given by Department management. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a network.

Don't attach County equipment of any kind to non-County computers or networks.

a member of the organization's information system support staff. Because it is a personnel function, a good choice would be an employee in an administrative position who is responsible for other routine personnel issues.

The User Responsibility Statement Administrator is responsible for the following tasks:

1. Identifying employees and other Users within the organization that will need to read and sign the Statement, as well as the relevant attachments.
2. Managing the signing process, including arranging for any briefings to be held in conjunction with Users signing the Statement and attachments.
3. Maintaining the signed Statements and attachments.
4. Ensuring that new employees and other new Users read and sign the basic Statement and any relevant attachments, and that the Department signing process is performed by all Users on an annual basis.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

SANTA CLARA COUNTY IT USER RESPONSIBILITY STATEMENT

This User Responsibility Statement establishes a uniform, County-wide set of minimum responsibilities associated with being granted access to Santa Clara County information systems and/or County networks. A violation of this Statement may lead to disciplinary action, up to and including termination.

Definitions

County information systems and networks include, but are not limited to, all County-owned, rented, or leased servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, data bases and software. These items are typically under the direct control and management of County information system support staff. Also included are information systems and networks under the control and management of a service provider for use by the County, as well as any personally-owned device that a User has express written permission to use for County business purposes.

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 the 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 constitutional provision, State or Federal statute, case law, or contract provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County-owned information system or on a network or system under the control and management of a service provider for use by the County.

A *mobile device* is any computing device that fits one of the following categories: laptops; Personal Digital Assistants (PDAs); handheld notebook computers and tablets, including but not limited to those running Microsoft Windows CE, PocketPC, Windows Mobile, or Mobile Linux operating systems; and "smart phones" that include email and/or data storage functionality, such as BlackBerry, Treo, Symbian-based devices, and iPhones. Note that the category "Mobile Device" does not include devices that are used exclusively for the purpose of making telephone calls.

A *public record* is any writing, including electronic documents, relating to the conduct of the people's business as defined by Government Code section 6252.

"*Remote access*" is defined as any access to County Information Technology (IT) resources (networks or systems) that occurs from a non-County infrastructure, no matter what technology is used for this access. This includes, but is not limited to, access to County IT resources from personal computers located in User's homes.

Users includes County employees who are on the permanent County payroll, as well as any

Key Points

permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home

1.6 No User, including information systems staff, may install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County system or network, without express written permission. All such connections must be approved in writing by the County Chief Information Officer (CIO) or designee. If authorized to install, configure or use such a device, the User must comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County systems.

Don't install or activate communication devices, such as modems, on County computers or networks.

1.7 The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.

Don't use encryption except when directed to do so.

1.8 Users must not attempt to elevate or enhance their assigned level of User privileges unless express written permission to do so has been granted by Department management. Users who have been granted enhanced privileges due to their specific jobs, such as system or network administrators, must not abuse these privileges and must use such privileges only in the performance of appropriate, legitimate job functions.

Don't attempt to enhance your assigned user privileges.

1.9 Users must use County-approved authentication mechanisms when accessing County networks and systems, and must not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by the County.

Don't attempt to disable or bypass County login procedures.

1.10 Users must not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or

Follow the terms of all software licensing agreements.

Key Points

installed, it is the responsibility of the User to check with Department management or information systems support staff.

1.11 All software on County systems must be installed by authorized systems support staff. Users may not download or install software on any County system unless express written permission has been obtained from Department management or authorized system support staff.

Don't download or install software without permission.

1.12 Loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business, is to be reported immediately to designated Department management, administrative, or systems support staff. Users are also expected to be aware of security issues, and are encouraged to report incidents involving breaches of security, such as the installation of an unauthorized device, or a suspected software virus.

Immediately report the loss or theft of computer equipment, and also report any suspected security incidents.

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

- Users must not access, or attempt to access, County systems or information unless specifically authorized to do so, *and* there is a legitimate business need for such access.

Don't access computers or data unless such access is related to your job.

- Users must not allow unauthorized individuals to use their assigned computer accounts; this includes the sharing of account passwords.

Don't share your user accounts or passwords with anyone.

- Users must not knowingly disclose County information to anyone who does not have a legitimate need for that information.

Don't share information with someone not entitled to have it.

- Users must take every precaution to ensure that all information classified as either Confidential or Restricted (or an equivalent classification) is protected from disclosure to unauthorized individuals.

Protect sensitive data from those not authorized to see it.

Key Points

- Users must not make or store paper or electronic copies of information unless it is a necessary part of that User's job.

Don't make copies of information unless this is required by your job.

1.14 Users must respect the importance of County- owned systems and data as a valuable asset, and should understand that any data stored or processed on any County computer, or transmitted over any County network, is County property. 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.

Don't change or delete data unless doing so is part of your job.

- Users must avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

Don't introduce computer viruses onto County computers.

- A User who leaves employment with the County must not retain, give away, or remove any County data or document from County premises, other than information provided to the public or copies of correspondence directly related to the terms and conditions of employment. All other County information in the possession of the departing User must be returned to the User's immediate supervisor at the time of departure.

When leaving County employment, don't take County data with you.

1.15 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 County technical support staff, other County Users, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County information system.

You should have no expectation of privacy for electronic data stored on County computers.

1.16 Users must respect all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, and confidential

Respect all intellectual property rights associated with data that you deal with while doing your job.

Key Points

information belonging to the County or any other third party.

1.17 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 User may use any County-owned network, computer system, or any other County-owned device or data for the following purposes:

- Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization

Don't use County computers to conduct your personal business.

- Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission

Don't use County computers for illegal activities.

- 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 but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business

Don't create or send demeaning or harassing material.

- To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business

Don't view, download, or send pornography or other potentially offensive materials.

- Knowingly propagating or downloading viruses or other malicious software

Don't download or transmit malicious software.

- Disseminating hoaxes, chain letters, or advertisements

Don't send chain letters.

1.18 Users that are employed by, or are otherwise associated with, a HIPAA impacted Department, are responsible for understanding and carrying out their responsibilities and duties as identified in the County HIPAA policies and procedures training, and other HIPAA-related materials that may be distributed from time to time.

Key Points

Handle all protected health information according to HIPAA regulations.

2. Internet and Email

The following items define the basic standards for use of County Internet and email resources. All Users of County information systems and networks are required to comply with these minimum standards.

2.1 In general, Users must not use County systems or networks for personal activities. However, reasonable incidental (*de minimus*) personal use of County resources, such as Internet access and email, is allowed as long as such use does not violate the County's acceptable use policies, and 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 what is considered appropriate incidental personal use, it is the responsibility of the User to ask for guidance from Department management.

Limit personal use of County computers.

2.2 When conducting County business, Users may not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by Department management. Such services include, but are not limited to, Internet Instant Messaging (such as AOL Instant Messaging), Internet email services (such as hotmail and gmail), peer-to- peer networking services (such as Kazaa), and social networking services (such as blogs, MySpace, Facebook and Twitter).

Don't use Internet email or data exchange services (such as FaceBook, MySpace, or other social networking sites) to conduct County business.

Key Points

2.3 It is the User's responsibility to become familiar with the specific County policies, procedures, and guidelines associated with the use of Internet-based communication and data exchange services. Users who have been granted permission to use an Internet-based communication or data exchange service for conducting County business are expected to adhere to all relevant County policies, procedures, and guidelines associated with the use of these services.

You are responsible for understanding County guidelines for using Internet data exchange services, such as social networking sites.

2.4 Users are responsible for understanding and following the County's policy with respect to the retention of email messages, including immediately deleting non-business related email messages once these messages have been read.

Follow County standards for retaining and deleting email messages.

2.5 Users may not use an internal County email account assigned to another individual to either send or receive email messages.

Don't use anyone else's email account.

2.6 Users may not configure their County email account so that it automatically forwards messages to an external Internet email system unless express written permission has been given by the Department Head. When automated forwarding is used, it must be for legitimate business purposes only, and is to be implemented with the User's full understanding of, and willingness to accept responsibility for, the associated risks for disclosure of sensitive information.

Don't automatically forward County email to an Internet email system.

3. Remote Access

The following items define the basic standards for remote access to County information systems and networks. All Users of County information systems and networks are required to comply with these minimum standards. Users actually granted remote access privileges must sign the statement provided as Attachment A.

Key Points

3.1 All remote access to County resources must be via the secure, centralized, County-controlled mechanisms and technologies approved by the County CIO or designee, and installed by authorized County systems support staff. Users are not permitted to implement, configure, or use any remote access mechanism other than the County-owned and managed remote access systems that have been formally approved and implemented by authorized system support staff.

Use only existing, approved County remote access systems.

3.2 Written approval for use of County remote access mechanisms is to be granted to a specific User by the appropriate Department Head or designee. Remote access to County resources will be implemented on a case-by-case basis based on job-related necessity, and only for those Users that have read and signed both the County's general User Responsibility Statement and the Remote Access agreement (Attachment A).

Get approval for all remote access to County systems.

3.3 Remote access sessions may be monitored and/or recorded, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County networks, systems, or data. Audit tools may be used to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

Remember that remote access sessions may be monitored and/or recorded.

3.4 All computer devices used to access County resources from a remote location must be configured according to County-approved security standards. These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by the County.

Computers used for remote access must be configured according to County standards.

3.5 Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, will

Key Points

take all reasonable measures to ensure that the device is protected from damage, access by third parties, loss, or theft. Loss or theft of such devices must be reported immediately to designated Department management or support staff.

Take measures to prevent the loss or theft of County-owned Mobile Devices used for remote access, and report loss or theft of such devices immediately.

3.6 Users will practice due diligence in protecting the integrity of County networks, systems, and data while remotely accessing County resources, and will immediately report any suspected security incident or concern to their Department management and IT support staff.

Take appropriate measures to protect County computers and data when using remote access.

3.7 Remote access sessions are subject to all other relevant County IT security policies and standards, including Local User Authentication (passwords), Data Classification, Internet Use, and Email.

When using remote access, continue to follow all County security policies.

4. Personally-Owned Devices

The following items define the basic standards for the use of personally-owned devices to conduct County business. All Users of County information systems and networks are required to comply with these minimum standards. Users actually granted the privilege of using a personally-owned device to conduct County business must also sign the statement provided as Attachment B. Note that in the case of Mobile Devices, the following provisions apply only to those devices that include email and/or data storage capability (such as BlackBerry devices and other "smart" phones), and do not apply to devices that are used strictly for the purpose of making telephone calls.

4.1 Use of personally-owned devices to conduct County business is prohibited unless express written permission is obtained from both the Department Head and IT Manager. If the User in question is a Department or Agency Head, express written permission must also be

Use of a personally-owned device to conduct County business requires approval.

Key Points

obtained from the County Chief Information Officer or designee. The use of personally-owned devices to conduct County business is a privilege, not a right, and employment at the County does not automatically guarantee the granting of this privilege.

4.2 The personally-owned device in question must use existing, County-approved and County-owned access/authentication systems when accessing County resources. Installation by Users of any hardware, software, or network interface components that provide unauthorized network connectivity, either wired or wireless, is prohibited.

If you are allowed to use your own computer or mobile device for County business, you must still use County-approved user login procedures.

4.3 The User shall allow the County to configure personally-owned devices as appropriate to meet security requirements, including the installation of specific security software that is mandated by County policy. When reasonably possible and practical, the County shall strive to provide a minimum of 24-hours notice to the User before configuring the personally-owned device. While the device is in the County's possession, the County shall not access, alter, retrieve or delete the User's personal information, communications, data, software or files stored on the device unless (a) it is reasonably necessary to do so to configure the device to meet security requirements, or (b) the User agrees to the specific access, alteration, retrieval or deletion.

You must allow authorized IT staff to configure, and periodically update, security software on any personally-owned device used to conduct County business.

4.4 Users authorized to use a personally-owned device must follow designated Department procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule. All software installations and updates are subject to verification by management-designated Department staff.

Follow Department procedures for updating and patching software on personally-owned devices.

4.5 Users have no expectation of privacy with respect to any County-owned communications, information, or files on any personally-owned device. Users agree that, upon request, the County may immediately access any and all work-related or County-owned communications, information or files stored on these devices, in order to ensure compliance with County policies. Except as otherwise provided in this policy or as required by law, the County shall not access any of the User's personal information, communications, data or files on the User's personally-owned devices.

The County has the right to access County data on any personally-owned device used to conduct County business.

4.6 Upon reasonable suspicion that a User has failed to comply with County policy, the County may search and access communications, information, data, or files on the personally-owned device that are reasonably related to the County's suspicion and interest in conducting the search. Any such search and access will take place with a goal of returning the device within 48 hours, if reasonably possible. The search and access shall be conducted in the presence of the User and/or the User's representative when requested by the User. At the request of the Department and with reasonable notice (not to exceed 48 hours), the User must provide a copy of all work-related or County-owned communications, information, or files stored on the personally-owned device. If the personally-owned device contains any information which is subject to lawful privilege (such as attorney-client or work product), that device shall be searched by Department representatives who are entitled to view the information, so that the privilege is not violated.

The County may search a personally-owned device if there is a suspicion that County policy has been violated.

4.7 If a user is contacted on a personally-owned device by someone from the County conducting County business, and the User has not obtained

Key Points September 2010

permission to conduct County business with that personally-owned device, then the County may not access that device regarding that User-received communication other than through legally permissible methods such as a subpoena, request for voluntary disclosure, etc. The preceding sentence shall not limit the County's right to direct a User to disclose the communication at issue upon reasonable notice.

The County will not require you to allow access to your personally- owned device for unsolicited, incoming County communications if that device has not been approved for use in conducting County business.

4.8 The User shall adhere to all relevant County security policies and standards, just as if the personally-owned device were County property. This includes, but is not limited to, policies regarding password construction and management, physical security of the device, device configuration, and hard drive sanitization prior to disposal. This does not restrict the User's personal use of the device so long as that personal use does not include or result in (a) the User's failure to adhere to all relevant County security policies and standards, or (b) the breach of the County's security policies or standards.

Even when using your own computer or other device for County business, you must still follow all County security policies.

Under most circumstances, you can continue to use an approved device for personal use as well as County business.

4.9 The User will make no modifications of any kind to operating system configurations implemented by the County on the device for security purposes, or to any hardware or software installed on the device by the County, without the express written permission of the County CIO's Office.

Don't modify any security configuration settings or security software on your computer.

4.10 The User must treat the device and the work-related or County-owned communications, information or files it contains as County property. The User must not allow access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by the County to access or use that data.

Treat any personally-owned device used for County business as if it were County-owned.

4.11 The User must immediately report to designated Department management or

Key Points

support staff any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the device, including loss or theft of the device.

Immediately report the loss or theft of a personally-owned device that has been used for County business.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

Key Points

Acknowledgement of Receipt

This Acknowledgement hereby incorporates the main body of the User Responsibility Statement. Attachments A and B are additional signature pages that apply only to those individuals that have been granted either remote access privileges (Attachment A) or permission to use a personally- owned device (Attachment B). These Attachments should only be signed if either of these conditions apply.

All Users must sign this Acknowledgement; Users with permission to use Remote Access should also sign Attachment A, and Users with permission to use personally- owned devices must complete and sign Attachment B.

The User should understand that the County's failure to enforce any provision of this Statement does not mean that the County will not enforce that or any other provision in the future. The User should also understand that if a clause, sentence or paragraph of this Statement is determined to be, invalid by a Court or County commission, this does not affect the validity of any other portion of the Statement.

By signing below, I acknowledge that I have read and understand all sections of the County of Santa Clara's User Responsibility Statement. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

Violation of any of the provisions in this User Responsibility Statement may result in disciplinary action.

If at any time, I have questions or doubts, or I feel ambivalent or unclear on any matter related to IT security and/or data confidentiality, I understand that it is my responsibility to request clarification from my supervisor or other appropriate manager before taking any action.

It is your responsibility to ask for clarification if you don't understand any aspect of the County IT security policy.

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

IT User Responsibility Statement Signature Page

I acknowledge that this Statement will still be in effect following a transfer to another County Agency or Department, and that all of its provisions will continue to apply to me as long as I am a County employee.

User Signature:

Print User Name:
Jason Volk

Agency/Department:

Date Signed:

EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

This page left intentionally blank.

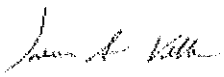
EXHIBIT I
VENDOR REMOTE ACCESS AND USER RESPONSIBILITY STATEMENTS

September 2010

Attachment A – Remote Access Signature Page

I have read and understand the contents of the User Responsibility Statement regarding Remote Access. I understand that violation of these provisions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

I received approval from my Department's management to be granted Remote Access privileges for legitimate County business, as evidenced by the signatures below.

User Signature:  Date: 11/25/2014
Printed User Name: Jason Volk

Agency/Department:

Agency/Department Manager Signature: Date:
Printed Manager Name:
Manager Title: