# 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


**FIRST AMENDMENT TO AGREEMENT 5500002508**
**BY AND BETWEEN THE COUNTY OF SANTA CLARA AND ALERTUS TECHNOLOGIES, LLC**

This is the First Amendment to the Agreement between the County of Santa Clara (County) and Alertus Technologies, LLC (CONTRACTOR) entered into on November 26, 2014 to provide Emergency Management Notification Software for the County.

This Agreement is amended as follows effective May 6, 2015:

1. Key Provisions, **CONTRACT VALUE**, of the Agreement is revised to read; "Contractor is entitled to reimbursement for the actual allowable expenditures subject to the provisions of this Agreement, not to exceed $66,550 which represents an increase of $6,800 from the prior not to exceed amount of $59,750".

2. Replace **Exhibit A Price Summary** with **Exhibit A1**, **Price Summary and Contacts** , as attached hereto and incorporated herein by this reference.

3. Replace **Exhibit I, Vendor Remote Access Agreement**, with **Exhibit I1**, **Vendor Remote Access Agreement** as attached hereto and incorporated herein by this reference.

All other terms and conditions of the Agreement remain in full force and effect. In the event of a conflict between the original Agreement and this Amendment, this Amendment controls.

Prepared and administered by: Alicia Jauregui, Buyer II at 408-491-7480 or Alicia.Jauregui@prc.sccgov.org

The Agreement as amended constitutes the entire agreement of the parties concerning the subject matter herein and supersedes all prior oral and written agreements, representations and understandings concerning such subject matter.

//

//

By signing below, signatory warrants and represents that he/she executed this Amendment 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 Amendment, the entity on behalf of which he/she acted, executed this Amendment.

| COUNTY OF SANTA CLARA | CONTRACTOR |
|---|---|
| 5/18/15 | By: Peter B. Lester |
| Julie Toy — Date | Print: Peter Lester |
| Procurement Manager | Title: National Accounts Manager - Healthcare |
| 5/20/15 | Date: May 18 2015 |
| Jenti Vandertuig — Date | |
| Director of Procurement | |

Attachments:
Exhibit A1- Price Summary and Contacts
Exhibit I1 - Vendor Remote Access Agreement

## EXHIBIT A1
## PRICE SUMMARY AND CONTACTS

### Section I - Additional Desktop Licenses per the 1st amendment

| Name of Deliverable: | Description: | Fixed Price: |
|---|---|---|
| Alertus Desktop Notification | Alertus Desktop Client application licensing | 2,000 @ $3.40 each |
| | TOTAL ONE TIME COST: | $6,800 |

### Section II – 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 |
| • Already purchased -TOTAL ONE TIME COST: | | $34,950.00 |

### Section III – 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 RECURRING COST | $24,800 |

*Maintenance and Support shall be paid at the anniversary date of each year.

**Section IV - 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 |

## Contacts

**County Contact:**
Bud Ramsey, (408) 793-6562
Bud.Ramsey@hhs.sccgov.org

**Vendor Contact:**
Peter Lester, (866) 425-3788 x706, plester@alertus.com
Ben Brewer, (866) 425-3788, bbrewer@alertus.com

## EXHIBIT I1
## Vendor Remote Access Agreement

The Agreement entered into _____ between Santa Clara County [Santa Clara Health & Hospital System] ("Customer") and Alertus ("Contractor") is hereby amended, effective _____, to add the following terms and conditions relating to Contractor's ability to remotely access Customer's systems as set forth below. In the event of any conflict or inconsistency between the applicable terms of this _____Amendment and the terms of the Agreement, the terms of the Agreement will apply and control in all instances.

### 1. Definitions

**County:** "County" shall mean Santa Clara County, in the State of California.

**Remote Access:** Remote access is the act of connecting to County systems from a non-County system through a public network or non-County network infrastructure. Systems include personal computers, workstations, servers and/or any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices).

### 2. Scope of Access

a. Customer hereby grants remote access to the following Customer systems at the locations listed, collectively referred to as "IS", in accordance with the terms of the Agreement and this Amendment:

Customer Systems: _____

All other access is prohibited.

b. Access is granted for the purpose of Contractor providing services and performing it's obligations as set forth in the Agreement including, but not limited to, supporting Contractor-installed programs. Unauthorized or illegitimate access to IS and/or County data/information is prohibited.

c. Modifications to Access Right: Customer will review the scope of Contractor's access rights periodically. In no instance will Contractor's access rights be reduced, limited or modified in any way that prevents or delays Contractor from performing it's obligations set forth in the Agreement. Any modifications to these access rights must be mutually agreed to in writing by Customer and Contractor.

### 3. Security Requirements

a. Contractor will not install any remote access capabilities on any Customer owned or managed system or network unless such installation and configuration is approved in writing by Customer's and Contractor's respective designees.

b. Contractor may only install and configure remote access capabilities on Customer systems in accordance with industry standard protocols and procedures, which must be reviewed and approved by Customer's designee.

c. Contractor may only remotely access County systems, including those connections initiated from a County system, if the following conditions are met:

1. Contractor will submit documentation verifying it's network security mechanisms to Customer for Customer's review and approval. Advanced written approval of Contractor's security mechanisms is required prior to Contractor being granted remote access.
2. Contractor security systems 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)), 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County site to Contractor site VPN infrastructure.

b. Centrally controlled authorizations (permissions) that are user specific (e.g., access lists that limit access to specific systems or LANs).

c. Audit tools that create detailed records/logs of access attempts.

d. All systems used to remotely access County systems must have installed and activated industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall).

e. Access must be established through a centralized collection of hardware and software centrally managed and controlled by Customer's and Contractor's respective designees.

**4. Monitoring/Audit**
Customer will monitor access to and activities on Customer owned or managed systems and networks. All remote access attempts to Customer networks and/or systems will be logged on a Customer managed and monitored system with the date, time, and user identification.

**5. Copying Deleting or Modifying Data**
Contractor is prohibited from copying, modifying, or deleting any data contained in or on any IS unless otherwise stated in the Agreement or unless Contractor receives prior written approval from Customer. This does not include data installed by the Contractor to fulfill it's obligations set forth in the Agreement.

**6. Connections to Non-County Networks and/or Systems**
Contractor agrees to make every effort to protect Customer's data contained on Customer owned and/or managed systems and networks within Contractor's control from unauthorized access. Prior written approval is required before Contractor may connect Customer networks or systems to non-Customer owned and/or managed networks or systems. Such connections shall be made in accordance with industry standard protocols and procedures as mutually agreed upon and shall be timely approved in writing by Customer. All modem access and other forms of remote access, such as but not limited to, Virtual Private Network (VPN) access, shall be made in accordance with mutually agreed upon industry standard protocols and procedures, which shall be timely approved in writing by the Customer.

**7. Term and Termination**
a. Term: The term of this Amendment will begin on it's effective date set forth above and will run co-terminous with the Agreement unless terminated earlier as set forth herein.

b. Termination: Customer may terminate this Amendment in accordance with the Termination section of the Agreement following Contractor's violation of any of the provisions set forth herein or in the Agreement.

**8. Person Authorized to Act on Behalf of Parties:** The following persons are the designees for purposes of this Amendment:
Contractor: Title/ Designee Peter Lester and/or Ben Brewer
Customer: 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.

**9. REMOTE ACCESS BACK-UP MODEL:**
This Remote Access Back-Up Model shall only be used in the event that the primary model selected below is inoperable. Contractor will abide by the additional provisions relating to the back up model selected below in the event Contractor utilizes the back up model.

**10. ACCESS MODELS:** Contractor agrees to abide by the following additional provisions relating to the primary model selected as indicated below. Please mark appropriate box for each model or if a model is inapplicable, please check the box marked N/A.

**A. VPN - Site-to-Site ☐Primary ☐Backup ☐ N/A**
Contactor support staff will have 24X7 access to all Contractor supported software, devices and systems (including applicable third party software products).

In addition to the above terms, the Contractor agrees to the following:

Only staff providing services or fulfilling Contractor obligations under the Agreement will be given remote access rights.

Only Contractor supported software, devices and systems (including applicable third party software products) will be accessed.

An encryption method reviewed and approved by the County will be used. Customer shall be solely responsible and liable for any delay or failure of Customer, 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.
Contractor will be required to log all access activity to the Customer. These logs will be kept for a minimum of 90 days and be made available to Customer no more frequently than once every 90 days.
Contractor will promptly report to Customer all system changes made via remote access.

**B. Client based VPN and SSLVPN County System Administrator Authentication ☐Primary ☐Backup ☐N/A**

A PIN number will be provided to the Contractor to use as identification for remote access. The Customer's [TITLE] or his/her designee will verify the PIN number provided by the Contractor. After verification the Customer [TITLE] or his/her designee will give the Contractor a one time password which will be used to authenticate Contractor when accessing the Customer's IS. All system changes will be subject to prior approval by Customer's [TITLE] or his/her designee. All remote access will be initiated only after a support case has been opened either by Customer or Contractor.

Because the PIN number allows access to privileged or confidential information residing on the Customer's IS, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment of a Contractor executive every time the PIN number is used.

In addition to the above terms, Contractor agrees to the following:

The PIN number is confidential, County-owned, and will be identified as such.

The PIN number must be kept in a secured environment under the direct control of the County, such as a locked office where public or other unauthorized access is not allowed.

The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.

If the PIN number is compromised or misused, the Contractor shall notify the Customer's [TITLE] or his/her designee within one (1) business day.

Contactors use the PIN number as part their normal business operations and for legitimate business purposes only. Use of the PIN number to gain unauthorized or illegitimate access to County information is prohibited and may result in contract termination and other potential consequences provided by law.

The PIN number will be issued to Contractor following execution of this Agreement.

The PIN number will be inactivated by the Customer's [TITLE] or his/her designee within five (5) business days following contract termination, or upon written request of the County for any reason.

C. **County-Controlled Enexity (Secure Link) Access** X **Primary Backup N/A**
The County-Controlled Enexity Access method involves using Securelink's Enexity tool installed in the County. County will establish a gateway where the vendor can access the designated software, devices and systems, within the County, as in Paragraph 1.b, from selected network-attached devices at the county site. County will control the access list for Vendors with access through Enexity gateways.

==========

**By executing this Amendment, both Contractor and Customer agree to abide by the terms and conditions contained herein.**

**Customer: Santa Clara County [Agency Name]**
**Name:** _____
**Title:** _____
**Date:** _____

**Name: Peter Lester and / /or Ben Brewer**
**Title: National Account Manager - Healthcare / / CISO**
**Date:** **May 18 2015**