Agreement Between Contractor:_____and
County of Santa Clara [Department of Employment & Benefit Services]

1. Definitions

a. Remote Access" is the act of accessing County Systems from a non-County network infrastructure.

b. "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

c. "County-owned information/data," for purposes of this Exhibit, 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 County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law 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 System or on a network or system under the control and management of a service provider for use by County.

d. "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

a. County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:

County System: Vocational Service & Appeals System (VSAS) and no others.

b. All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.

c. Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the Designated Systems.

d. County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

a. Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets or exceeds NIST 800-53 standards, or an equivalent industry standard.

b. Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:

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

(i) Upon request by an authorized County representative, Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County reserves the right to advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.

(ii) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:

(aa) 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.

(bb) County personnel will control authorizations (permissions) to specific systems or networks.

(cc) 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.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include 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 County System 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 set forth in the Agreement.

6. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet or exceed NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

7. Person Authorized to Act on Behalf of Parties: The following persons are the designees for purposes of this Agreement:

Contractor:
County: Kalu Igwe-Kalu, kalu.igwe-kalu@ssa.sccgov.org

Either party may change the aforementioned names and or designees by providing the other party with no less than three (3) business day's prior written notice.

8. Additional Requirements

Contractor agrees to the following:

a. Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.
b. Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.
c. An encryption method that meets or exceeds Federal Information Processing Standard (FIPS) Publication 140-2 will be used.
d. Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall report any suspected security incident or concern to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.
e. Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.
f. Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.
g. Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees shall report loss or theft of such devices to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

9. 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. The remote access solution must conform to County policy and security requirements.
b. 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 not applicable, please check the button marked N/A).

(i) VPN Site-to-Site ☐ Primary ☐ Backup ■ N/A

The VPN Site-to-Site method involves a VPN concentrator at both the Contractor 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 Systems from selected network-attached devices at the Contractor site.

(ii) 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.

An Authentication Token (a physical device or software token that an authorized remote access user is given for user authentication purposes, such as a CryptoCard, RSA token, SecureAuth IdP, Arcot software token, or other such one-time-password mechanism approved by the County Information Security Office) will be issued to the Contractor in order to authenticate Contractor staff when accessing County Designated Systems via this method. The Contractor agrees to the following when issued an Authentication Token:

a. Because the Authentication Token allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the Authentication Token as it would a signature authorizing a financial commitment on the part of the Contractor.

b. A hardware Authentication Token is a County-owned physical device, and will be labeled as such. The label must remain attached at all times.

c. The Authentication Token is issued to an individual employee of the Contractor and may only be used by the designated individual.

d. The Authentication Token must be kept in the possession of the individual Contractor employee it was issued to or 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 Authentication Token will be kept under Contractor control.

f. If the Authentication Token is misplaced, stolen, or damaged, the Contractor will notify the County TechLink Center by phone within 24 hours.

g. Contractor agrees to use the Authentication Token as part of its normal business operations and for legitimate business purposes only.

h. The Authentication Token will be issued to Contractor following execution of this Agreement. Hardware Authentication Tokens will be returned to the County's Tech Link Center within five (5) business days following contract termination, or upon written request of the County for any reason.

i. Contractor will notify the County's the County TechLink Center within one working day of any change in personnel affecting use and possession of the Authentication Token. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org. Contractor will obtain the Authentication Token from any employee who no longer has a legitimate need to possess the Authentication Token. The County will recoup the cost of any lost or non-returned hardware Authentication

j. Contractor will not store account or password documentation or PINs with Authentication Tokens.

k. Contractor will ensure all Contractor employees that are issued an Authentication Token will be made aware of and provided with a written copy of the requirements set forth in this Addendum.

(iii) 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 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 Designated Systems, the Contractor must first notify the County's Remote Access Contact.

The County's TechLink Center 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 Designated Systems. Contractor agrees to the following:

a. Because the PIN number allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.

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

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

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.

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

f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.

g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to Designated Systems, other County Systems, and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.

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

i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

(iv) County-Controlled Enexity Access ☐ **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 Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through Enexity gateways.

Signatures of Contractor Employees receiving Authentication Tokens (**Only for VPN Client Access and if tokens issued by County**).

Contractor: _____
[TYPE NAME HERE]

Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]

For multiple Contractor Signatures, please use page 6.

Contractor: _____
[TYPE NAME HERE]

Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]

Contractor: _____
[TYPE NAME HERE]

Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]

Contractor: _____
[TYPE NAME HERE]

Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]

Contractor: _____
[TYPE NAME HERE]

Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]