Agreement Between [Community Partner/Contractor: _____ and Santa Clara County [Department of Employment & Benefit Services]

Dated [Date]: _____

1. Scope of Access

a. Remote access is the act of connecting to County of Santa Clara ("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). County hereby grants remote access to the following County systems at the locations listed collectively referred to as "IS," in accordance with the terms of the Agreement:

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

All other access is prohibited.

b. Access is granted for the purpose of Community Partner/Contractor providing services and performing its obligations as set forth in the Agreement including, but not limited to, supporting Community Partner/Contractor-installed programs. 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 penalty allowed by law.

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

2. Security Requirements

a. Community Partner/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 Community Partner/Contractor respective designees.

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

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

1. Community Partner/Contractor will submit documentation verifying its network security mechanisms to County for County's review and approval. The County requires advanced written approval of Contractor's security mechanisms prior to Community Partner/Contractor being granted remote access.

2. Community Partner/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)); or 3) something you are (e.g., fingerprints, retina scan).

The only exceptions are County approved County site to Community Partner/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 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 County's and Community Partner/Contractor's respective designees.

3. Monitoring/Audit

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

4. Copying Deleting or Modifying Data

Community Partner/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 County. This does not include data installed by the Contractor to fulfill its obligations set forth in the Agreement.

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

Community Partner/Contractor agrees to make every effort to protect County's data contained on County owned and/or managed systems and networks within Community Partner/Contractor's control from unauthorized access. Prior written approval is required before Community Partner/Contractor may connect County networks or systems to non-County owned and/or managed networks or systems. Such connections will be made in accordance with industry standard protocols and procedures as mutually agreed upon and will be timely approved in writing by County. All modem access and other forms of remote access, including, but not limited to, VPN access, will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County.

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

Community Partner/Contractor: Title/ Designee _____
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 day's prior written notice.

7. REMOTE ACCESS BACK-UP MODEL:

This Remote Access Back-Up Model will only be used in the event that the primary model selected below is inoperable. Community Partner/Contractor will abide by the additional provisions relating to the backup model selected below in the event Community Partner/Contractor utilizes the backup model.

8. ACCESS MODELS:

Community Partner/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

Community Partner/Contractor 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 Community Partner/Contractor agrees to the following:

1. Only staff providing services or fulfilling Community Partner/Contractor obligations under the Agreement will be given remote access rights.
2. Only Community Partner/Contractor supported software, devices and systems (including applicable third party software products) will be accessed.
3. 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 Community Partner/Contractor where such delay or failure causes Community Partner/Contractor to fail to meet or perform, or be delayed in meeting or performing, any of its obligations under the Agreement.
4. Community Partner/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.
5. 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.
6. Community Partner/Contractor will promptly report to Customer all system changes made via remote access.

B. Manually Switched Dialup Modem ☐ Primary ☐ Backup ☐ N/A

In addition to the terms set forth elsewhere in this Agreement, the Community Partner/Contractor agrees to the following:

1. Community Partner/Contractor will use reasonable efforts to notify the County's Technical Services Manager or his/her designee in the following instances: at least ½ hour prior to access to allow County to activate the modem connection and give estimated time connection will be required and when the access can be deactivated.

2. County acknowledges that Community Partner/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 this Remote Access Back-Up Model.

3. County is solely responsible and liable for any inability or delay in Community Partner/Contractor performing its obligations under the Agreement where such inability or delay is caused by the use of this Remote Access Back-Up Model.

4. 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.

C. Client Based VPN/SSLVPN CRYPTOCard Authentication ☐ Primary ☐ Backup ☐ N/A

This equipment, known as the CRYPTOCard, is a product used to establish authentication of the Community Partner/Contractor when accessing the Customer's facility through County provided VPN and/or SSLVPN capabilities.

Because the CRYPTOCard allows access to privileged or confidential information residing on the County's IS, the Community Partner/Contractor agrees to treat the CRYPTOCard as it would a signature authorizing a financial commitment of a Community Partner/Contractor every time the CRYPTOCard is used.

In addition to the above terms, the Community Partner/Contractor agrees to the following:

1. The CRYPTOCard is a County-owned device, and will be labeled as such. The label must remain attached at all times.

2. The CRYPTOCard must be kept in a secured environment under the direct control of the Community Partner/Contractor, such as a locked office where public or other unauthorized access is not allowed.

3. If the remote access equipment is moved to a non-secured site such as a repair location, the CRYPTOCard will be kept under Community Partner/Contractor control.

4. The CRYPTOCard is issued to an individual employee of the Community Partner/Contractor and may only be used by the designated individual.

5. If the CRYPTOCard is misplaced, stolen, or damaged, the Community Partner/Contractor will notify County by phone within one (1) business day. The County contact is the County's [TITLE] or his/her designee.

6. Community Partner/Contractor uses the CRYPTOCard as part their 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.

7. The CRYPTOCard will be issued to Community Partner/Contractor following execution of this Agreement. The CRYPTOCard will be returned to the County's [Help Desk or _____ or his/her designee within five (5) business days following contract termination, or upon written request of the County for any reason. Community Partner/Contractor will notify County's [Help Desk or _____ or his/her designee within one working day of any change in personnel affecting use and possession of the CRYPTOCard. Community Partner/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 Community Partner/Contractor in the amount of $300 per card.

8. Community Partner/Contractor will not store password documentation with CRYPTOCards.

9. Community Partner/Contractor agrees that all employees, agents, contractors, s 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.

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

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

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

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

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

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

3. If the remote access equipment is moved to a non-secured site such as a repair location, the PIN number will be kept under Community Partner/Contractor control.

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

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

6. Community Partner/Contractor use the PIN number as part their 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.

7. The PIN number will be issued to Community Partner/Contractor following execution of this Agreement.

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

Community Partner/Contractor: _____
[TYPE NAME HERE]

Community Partner/Contractor Signature: _____

_____ Date: _____
[TITLE]

_____ Contact Phone: _____
[OFFICE LOCATION]

For multiple Community Partner/Contractor Signatures, please use page 6.

Community Partner/Contractor: ______________________________
[TYPE NAME HERE]

Community Partner/Contractor Signature: ______________________________

______________________________ Date: ______________________________
[TITLE]

______________________________ Contact Phone: ______________________________
[OFFICE LOCATION]

Community Partner/Contractor: ______________________________
[TYPE NAME HERE]

Community Partner/Contractor Signature: ______________________________

______________________________ Date: ______________________________
[TITLE]

______________________________ Contact Phone: ______________________________
[OFFICE LOCATION]

Community Partner/Contractor: ______________________________
[TYPE NAME HERE]

Community Partner/Contractor Signature: ______________________________

______________________________ Date: ______________________________
[TITLE]

______________________________ Contact Phone: ______________________________
[OFFICE LOCATION]

Community Partner/Contractor: ______________________________
[TYPE NAME HERE]

Community Partner/Contractor Signature: ______________________________

______________________________ Date: ______________________________
[TITLE]

______________________________ Contact Phone: ______________________________
[OFFICE LOCATION]