SERVICE AGREEMENT

This Agreement is made and entered into on this day of **April 15, 2020** by and between the **Workforce Development Board of Solano County** (WDB) and **NETXPERTS, INC.** herein known as (VENDOR).

1. **TERM OF AGREEMENT**
The term of this Agreement is twelve (12) months. Services shall commence on **April 15, 2020** through **April 30, 2021** after completion of all signatures. The Agreement will remain in full force and effect until the completion of the Scope of Work as described in Exhibit A of this Agreement.

2. **SCOPE OF SERVICES**
The VENDOR shall provide the specified deliverables as described in the scope of work which shall be incorporated as Exhibit A-Scope of Work of this Agreement.

3. **COMPENSATION**
3.1. Rate: VENDOR will be compensated at a rate of **$4,700.00** per month.

3.2. Amount: VENDOR will be compensated not to exceed **$56,400.00**

3.3. Invoicing and Timing of Payment: Payment will be made according to the following terms:

3.3.1. VENDOR shall submit monthly invoices detailing work performed for each deliverable detailed in the Scope of Work and amount payable to the WDB's One Stop Senior Manager. The payment shall be made only after the services required under this contract have been performed to the satisfaction of the Executive Director/President, and the deliverables described in Exhibit A have been accepted in writing by the Executive Director/President OR his/her designee.

3.3.2. The VENDOR may be asked to perform special tasks or projects separate from the Scope of Work. Prior written approval by WDB will be required if any services are performed by the VENDOR that are not specified in Exhibit A – Scope of Work and a separate invoice will be submitted by the VENDOR.

3.3.3. The VENDOR shall provide any additional documentation as required by WDB at any time in order to substantiate VENDOR claims for payment. WDB may elect to withhold payment for failure by VENDOR to provide such documentation required by WDB.

3.3.4. The VENDOR agrees that the total maximum compensation for the services performed will not exceed the amount individually assigned in each Scope of Work Order (task order). The VENDOR agrees that any work performed above and beyond this amount will be gratis and will not be billed to the WDB.

3.3.5. Tax Withholding: Payment to non-California resident or nonresident alien VENDOR performing services in California may be reduced by any required state tax withholding or federal tax withholding or both.

4. **REPRESENTATIONS**
4.1. WDB relies upon VENDOR's professional ability and training as a material inducement

to enter into this Contract. VENDOR represents that VENDOR will perform the work according to generally accepted professional practices and standards and the requirements of applicable federal, state and local laws. WDB's acceptance of VENDOR's work shall not constitute a waiver or release of VENDOR from professional responsibility.

4.2. VENDOR further represents that VENDOR possesses current valid appropriate licensure, including, but not limited to driver's license, professional license, certificate of tax-exempt status, or permits, required to perform the work under this Contract.

5. INSURANCE

5.1. Workers' Compensation: The VENDOR assumes full responsibility for maintaining adequate workers' compensation and disability insurance coverage for the VENDOR or any agents or employees performing services for the VENDOR under the terms of this Agreement, if applicable.

5.2. Without limiting VENDOR's obligation to indemnify WDB, VENDOR must procure and maintain for the duration of the Contract insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work under this Contract and the results of that work by VENDOR, VENDOR's agents, representatives, employees or subcontractors.

5.2.1. Minimum Scope of Insurance: Coverage must be at least as broad as: Insurance Services Office Commercial General Liability coverage (occurrence Form CG 00 01)

- Insurance Services Office Form Number CA 00 01 covering Automobile Liability, code 1 (any auto)
- Workers' Compensation insurance as required by the State of California and Employer's Liability Insurance.

5.2.2. Minimum Limits of Insurance: VENDOR must maintain limits no less than

1. General Liability: (Including operations, products and completed operations.)	**$1,000,000**	per occurrence for bodily injury, personal injury and property damage, or the full per occurrence limits of the policy, whichever is greater. If Commercial General Liability insurance or other form with a general aggregate limit is used, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.
2. Automobile Liability: Aggregate	**$1,000,000** **$2,000,000**	per accident for bodily injury and property damage
3. Workers' Compensation		as required by the State of California
4. Employers Liability Aggregate	**$1,000,000** **$2,000,000**	per accident for bodily injury of disease.

Additional Insurance Coverage: To the extent coverage is applicable to VENDOR's services under this VENDOR, VENDOR must maintain the following insurance coverage:

1. Cyber Liability:	**$1,000,000**	per incident with the aggregate limit of twice the required limit
2. Professional Liability: Aggregate	**$1,000,000 $2,000,000**	combined single limit per claim and in the aggregate. The policy shall remain in full force and effect for no less than 3 years following the completion of work under this Contract.

5.3. Minimum Limits of Insurance: VENDOR must maintain limits no less than

5.4. If VENDOR maintains higher limits than the minimums shown above, WDB is entitled to coverage for the higher limits by VENDOR.

5.5. Deductibles and Self-Insured Retentions: Any deductibles or self-insured relations must be declared to and approved by the WDB. At the option of the WDB, either:

5.5.1. The insurer will reduce or eliminate such deductibles or self-insured retentions with respect to WDB, its officers, officials, agents, employees and volunteers; or;

5.5.2. VENDOR must provide a financial guarantee satisfactory to WDB guaranteeing payment of losses and related investigations, claim administration, and defense expenses.

5.6. Other Insurance provisions: The general liability and automobile liability policies must contain, or be endorsed to contain, the following provisions:

5.6.1. The WDB of Solano County, its officers, officials, agents, employees, and volunteers must be included as additional insured with respect to liability arising out of automobiles owned, leased, hired or borrowed by or on behalf of VENDOR; and with respect to liability arising out of work or operations performed by or on behalf of VENDOR including materials, parts or equipment furnished in connection with such work or operations. General Liability coverage shall be provided in the form of an Additional Insured endorsement. The insurance afforded to the additional insured shall be at least as broad as that afforded to the first named insured.

5.6.2. For any claims related to work performed under this Contract, VENDOR's insurance coverage must be primary insurance with respect to the WDB of Solano County, its officers, agents, employees, or volunteers is excess of VENDOR's insurance and shall not contribute to it.

5.6.3. Should any of the above described policies be cancelled prior to the policies' expiration date, VENDOR agrees that notice of cancellation will be delivered in accordance with the policy provisions.

6. WAIVER OF SUBROGATION

6.1. VENDOR agrees to waive subrogation which any insurer of VENDOR may acquire from VENDOR by virtue of the payment of any loss. VENDOR agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation.

6.2. The Workers' Compensation policy must be endorsed with a waiver of subrogation in favor of the WDB for all work performed by VENDOR, its employees, agents and subcontractors.

7. **ACCEPTABILITY OF INSURERS**
Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A:VII unless otherwise acceptable to the WDB.

8. **VERIFICATION OF COVERAGE**
   - **8.1.** Contractor must furnish WDB with original certificates and endorsements effecting coverage required by this Contract. The endorsements should be on forms provided that conform to the WDB's requirements and acceptable to the WDB.
   - **8.2.** WDB must receive and approve all certificates and endorsements before work commences.
   - **8.3.** However, failure to do so shall not operate as a waiver of these insurance requirements.
   - **8.4.** WDB reserves the right to require complete, certified copies of all required insurance policies, including endorsements affecting the coverage required by these specifications at any time.

9. **INDEPENDENT VENDOR**
   - **9.1.** VENDOR is an independent vendor and not an agent, officer or employee of the WDB. The parties mutually understand that this Agreement is between two independent contractors and is not intended to and shall not be construed to create the relationship of agent, servant, employee, partnership, joint venture or association.
   - **9.2.** VENDOR shall have no claim against WDB for employee rights or benefits including, but not limited to, seniority, vacation time, vacation pay, sick leave, personal time off, overtime, medical, dental or hospital benefits, retirement benefits, Social Security, disability, Workers' Compensation, unemployment insurance benefits, civil service protection, disability retirement benefits, paid holidays or other paid leaves of absence.
   - **9.3.** VENDOR is solely obligated to pay all applicable taxes, withholding, Social Security, unemployment, disability insurance, Worker's Compensation and Medicare payments.
   - **9.4.** VENDOR shall indemnify and hold WDB harmless from any liability which WDB may incur because of VENDOR'S failure to pay such obligations, as set forth in this paragraph.
   - **9.5.** As an independent contractor, VENDOR is not subject to the direction and control of the WDB except as to the final result contracted for under this Agreement. WDB may not require VENDOR to change VENDOR'S manner of doing business, but may require redirection of efforts to fulfill this Agreement.
   - **9.6.** VENDOR may provide services to others during the same period VENDOR provides service to WDB under this Agreement.
   - **9.7.** Any third persons employed by VENDOR shall be under VENDOR's exclusive direction, supervision and control. VENDOR shall determine all conditions of employment including hours, wages, working conditions, discipline, hiring and discharging or any other condition of employment.
   - **9.8.** As an independent contractor, VENDOR shall indemnify and hold WDB harmless from any claims that may be made against WDB based solely on the contention by a third party that an employer-employee relationship exists under this Agreement Notwithstanding this provision, to the extent that any claim, as described in this subsection, is based on alleged negligence or willful misconduct of WDB, VENDOR shall have no duty to indemnify and hold WBD harmless for that particular claim.
   - **9.9.** VENDOR with full knowledge and understanding of the foregoing, freely, knowingly, willingly and voluntarily waives the right to assert any claim to any right or benefit or

term or condition of employment insofar as they may be related to or arise from compensation paid hereunder.

10. CONFIDENTIALITY

10.1. All nonpublic data and information submitted or made available to VENDOR by the WDB, and other work developed by VENDOR under this Agreement, must be utilized by VENDOR in connection with this Agreement only, and must not be made available to any other sources.

10.2. VENDOR shall prevent unauthorized disclosure of names and other client-identifying information, except for statistical information not identifying a particular client receiving services under this Agreement. VENDOR shall not use client specific information for any purpose other than carrying out VENDOR's obligations under this Agreement.

10.3. Except as otherwise permitted by this Agreement or authorized by law, VENDOR shall not disclose any confidential information to anyone other than the State of California without prior written authorization from the WDB.

10.4. For purposes of this section, identity shall include, but not be limited to, name, identifying number, symbol or other client identifying particulars, such as fingerprints, voice print or photograph. Client shall include individuals receiving services pursuant to this Agreement.

11. DISCLOSURE OF DOCUMENTS

VENDOR must not disclose any of WDB's properly marked confidential documents without written authorization, unless disclosure is required by law.

12. BUSINESS OWNERSHIP

The WDB owns the hardware, cloud-based services and subscription services and will maintain full access to it. This means the WDB will have a record of/ access to all current log-on / username and password information. Any changes to system access must be provided to the WDB. Only industry standard hardware and software products are acceptable for use with WDB systems. This contract covers labor only. All hardware / software purchases are generally made by the WDB.

13. OWNERSHIP OF WORK PRODUCT

All documents or other information developed as part of this Agreement or received by VENDOR become the property of WDB and must be made available to WDB upon demand or termination of this Agreement. Should copyrights of any of the products be deemed necessary in this project by mutual Agreement, such copyright shall be held by WDB and made available to the general public. The VENDOR shall be responsible for obtaining all necessary legal releases for use of any third-party proprietary materials.

14. ADVERTISEMENT

VENDOR may not use the name WDB or any variation thereof for advertising or publicity purposes without first obtaining the written consent of WDB.

15. LIMITATIONS UPON SUBCONTRACTING AND ASSIGNMENT

The VENDOR assumes full responsibility for any entity that is procured to perform the specified services in Exhibit A – Scope of Work. This Agreement may not be assigned voluntarily or by operation of law, without the prior written approval of WDB.

16. VENDOR'S PERSONNEL

16.1. VENDOR agrees that all work to be performed under this Agreement will be performed by VENDOR. The VENDOR agrees that no portion of the work to be performed under this Agreement will be subcontracted to a third party or performed by other VENDOR employees not having the required documents and signed Exhibit B - Use and Confidentiality of Participant Personally Identifiable Information policy. In addition. VENDOR shall not subcontract any work under this Agreement nor assign this Agreement or monies due without the prior written consent of the WDB's One Stop Services Manager, applicable Division Manager or his her designee and the President/Executive Director subject to any required state or federal approval.

16.2. If WDB consents to the use of subcontractors, VENDOR shall require and verify that its subcontractor maintain insurance meeting all of the requirements stated in Section 5, "Insurance" above.

16.3. Assignment by VENDOR of any monies due shall not constitute an assignment of the Agreement.

16.4. Any third persons employed by VENDOR shall be under VENDOR 's exclusive direction, supervision and control. VENDOR shall determine all conditions of employment including hours, wages, working conditions, discipline, hiring and discharging or any other condition of employment.

16.5. Employees of VENDOR must carry out the performance of the services contracted for under this Agreement. VENDOR must, at its own expense, provide all personnel necessary to perform the services. VENDOR warrants that all personnel engaged in the services are qualified to perform the services and must be properly licensed and otherwise authorized to do so under all applicable laws.

17. DEFAULT

17.1. If VENDOR defaults in VENDOR'S performance, WDB shall promptly notify VENDOR in writing. If VENDOR fails to cure a default within 30 days after notification or if the default requires more than 30 days to cure and VENDOR fails to commence to cure the default within 30 days after notification, then VENDOR'S failure shall terminate this Contract.

17.2. If VENDOR fails to cure default within the specified period of time, WDB may elect to cure the default and any expense incurred shall be payable by VENDOR to WDB.

17.3. If WDB serves VENDOR with a notice of default and VENDOR fails to cure the default, VENDOR waives any further notice of termination of this Contract.

17.4. If this Contract is terminated because of VENDOR'S default, WDB shall be entitled to recover from VENDOR all damages allowed by law.

18. INDEMNIFICATION

18.1. VENDOR must release, defend, indemnify, hold harmless and assume the defense of WDB, Solano County, State of California, and the United States Department of Labor (DOL) its officers, employees, agents and board members from all claims, losses,

damages, including property damages, personal injury, death and liability of every kind, directly or indirectly arising from VENDOR'S operations or from any persons directly or indirectly employed by, or acting as agency for, VENDOR, excepting the negligence or willful misconduct of the WDB. This indemnification shall extend to claims, losses, damages, injury and liability for injuries occurring after completion of VENDOR's services, as well as during the progress of rendering such services.

18.2. Acceptance of insurance required by this Agreement does not relieve VENDOR from liability under this indemnification clause. This indemnification clause shall apply to all damages or claims for damages suffered by VENDOR's operations regardless if any insurance is applicable or not.

19. CHANGES AND AMENDMENTS

19.1. WDB may request changes in VENDOR'S scope of work. Any mutually agreed upon changes, including any increase or decrease in the amount of VENDOR'S compensation, shall be effective when incorporated in written amendments to this Agreement.

19.2. The party desiring the revision shall request amendments to the terms and conditions of this Agreement in writing. Any adjustment to this Agreement shall be effective only upon the parties' mutual execution of an amendment in writing.

19.3. No verbal agreements or conversations prior to execution of this Agreement or requested amendment shall affect or modify any of the terms or conditions of this Agreement unless reduced to writing according to the applicable provisions of this Contract.

20. SERVICE AGREEMENT EXTENSION

Unless terminated by either party prior to March 31, 2021, this Agreement shall automatically extend from April 1, 2021 through March 31, 2022 to allow for continuation of services and sufficient time to complete novation or renewal agreement.

21. ENTIRETY OF AGREEMENT

This service Agreement, including any exhibits referenced, constitutes the entire Agreement between the parties and there are no inducements, promises, terms, conditions or obligations made or entered into by WDB or VENDOR other than those contained in it.

22. INTERPRETATION

This Agreement must be interpreted as though prepared by both parties.

23. PRESERVATION OF AGREEMENT

Should any provision of this Agreement be found invalid or unenforceable, the decision will only affect the provision interpreted, and all remaining provisions will remain enforceable.

24. TERMINATION OF AGREEMENT

This Agreement may be terminated by the WDB or VENDOR, at any time with or without cause, upon 30 days written notice from one to the other. The WDB may terminate this Agreement immediately upon notice of VENDOR's malfeasance. The VENDOR may retain amounts, if any, paid by WDB under this Agreement prior to termination, but explicitly waives any right to additional amounts of any kind. In the event of termination, WDB shall be liable

for payment only for the products delivered and acceptable prior to the effective date of termination.

25. CALIFORNIA LAW

This Agreement must be construed in accordance with the laws of the State of California. Any action commenced about this Agreement must be filed in the Solano County Superior Court.

26. AUTHORITY TO EXECUTE

The persons executing this Agreement on behalf of the parties warrant that they are duly authorized to execute this Agreement and that by executing this Agreement, the parties are formally bound.

27. WAIVER

Any failure of a party to assert any right under this Agreement shall not constitute a waiver or a termination of that right, under this Agreement or any of its provisions.

Exhibit A: Scope of Work
Exhibit B: Use and Confidentiality of Participant Personally Identifiable Information Policy

VENDOR certifies by signing this Agreement that neither it nor its principals are currently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any federal department or agency.

IN WITNESS THEREOF, the parties have executed this Agreement on the day and year shown below.

APPROVED BY THE VENDOR

Signature: _____ Date: 4/15/2020
(Signature, Contractor's Duly Authorized Representative)
Name: GARY NORDINE
Title: CEO
Address: 1777 BOTELHO DR STE 102 WALNUT CREEK 94596
Phone No. 925-806-0800

APPROVED BY THE WORKFORCE DEVELOPMENT BOARD OF SOLANO COUNTY

Signature: Heather Henry Date: 4/30/2020
(Signature, Contractor's Duly Authorized Representative)
Name: Heather Henry
Title: President/Executive Director

Approved as to Form: Bernadette S. Curry
Solano County Counsel

Exhibit A
Scope of Work

A. VENDOR RESPONSBILITIES

1. AVAILABILITY TO PERFOM SERVICES

Vendor will:

i. Provide and train all qualified staff in order to plan for and administer the contracted services;
ii. Provide services for duration of contract; and,
iii. Provide services during scheduled days and/or hours as appropriate.

2. SERVICE ACTIVITIES

Vendor will:

i. On-Boarding

a. Serve at WDB's Managed IT Systems vendor to provide maintenance and support to WDB's network infrastructure, hardware and software.
b. Conduct an initial evaluation of WDB's current network infrastructure system, at the Fairfield and Vallejo sites, to assess and identify risks and potential deficiencies within the system.
c. Work in tandem with WDB's interim IT Systems vendor to transition all licenses, materials, in-progress tasks, etc., and obtain any necessary information pertinent to maintaining the network infrastructure.
d. Provide ongoing support, necessary training(s), and guidance to WDB and designated staff throughout the duration of the Agreement.
e. Communicate periodically with the interim IT provider, on an as needed basis.

ii. Software & Equipment

a. Maintain all cloud-based network services.
b. Maintain network security, firewall and content filtering systems.
c. Perform router management.
d. Maintain virus detection, protection and removal products.
e. Manage spyware.
f. Perform software updates and patches.
g. Perform hardware and software preventative maintenance.
h. Perform hardware and software troubleshooting.
i. Maintain the WDB's product of licensing.
j. Monitor data back-up's and perform data recovery, if needed.
k. Provide ongoing help desk and technical support.
l. Provide remote support to WDB, as needed.
m. Maintain physical presence through regular on-site visits; dates to be determined by the Vendor and WDB.

n. Make recommendations about planning for efficiency and maintaining current products with industry standard products.
o. Document hardware and/or software changes.
p. Provide vendor-documented instructions, templates, etc., to use in order to perform select functions which include, but are not limited to, creating a new user account to log onto the network, creating a new email account, disabling an email account.
q. Make disaster recovery planning recommendations.
r. Provide monthly report on work accomplished, work in progress and work to be completed.

B. RESPONSE TIME – On Call and Emergency Services

VENDOR shall perform all scheduled work during the normal business hours of Monday through Friday, 8:00am – 5:00pm PT or as outlined by WDB. All services must be provided in a manner not to disrupt normal business hours.

C. ADMINSTRATION

1. **Maintenance of Effort**
   VENDOR assures that services provided, and funds received under this Agreement will not supplant existing services or funds allocated for the same purpose.

2. **Successors**
   Should the VENDOR sell or otherwise relinquish all or any portion of the ownership of the VENDOR Corporation during the course of this Agreement, any future owner(s) of the corporation will agree to be bound by the provisions stipulated herein for the length of the contract.

3. **Time is of the Essence of this Agreement**
   All services to be performed specified under this Agreement including training must be delivered on or before the ending of date of this Agreement.

EXHIBIT B

WORKFORCE DEVELOPMENT BOARD
OF SOLANO COUNTY

POLICY ISSUANCE

Date: May 18, 2018 Number: 2018-01

USE AND CONFIDENTIALITY OF PARTICIPANT PERSONALLY IDENTIFIABLE INFORMATION (PII)

INTRODUCTION

It is the policy of the Workforce Development Board of Solano County (WDB) to protect the privacy of all applicants for program services, as well as the privacy of all customers and clients receiving program services. The purpose of this policy is to describe how the WDB will protect all personally identifiable information (PII) on applicants and customers, and the consequences for not adhering to these safeguards.

Under the Workforce Innovation and Opportunity Act (WIOA), staff obtains personal and confidential information from individuals as part of eligibility determination and continuation of services. WIOA and other federal and state regulations governing information sharing stipulate implementation of confidentiality policies and procedures.

Personal information will be treated in the strictest confidence and will not be shared outside of the WDB without written authorization, except for auditing purposes and other grantor-imposed information-sharing requirements. The purpose of this policy is to specify the requirements for the use, storage, and security of sensitive and confidential information.

QUESTIONS

Questions relating to this policy should be directed to Tracy White, One-Stop Manager, at twhite@solanowdb.org or at 707-863-3520.

ATTACHMENTS

- Attachment A: Staff/Representative Confidentiality Agreement
- Attachment B: Participant Confidentiality Rights
- Attachment C: Definition of Key Terms

POLICY

Employees, contractors, consultants, and volunteers of WDB (herein "staff and representatives") may be exposed to participant information which is confidential and/or privileged and proprietary in nature. As part of grant activities, staff and representatives may have access to large quantities of personally identifiable information (PII) relating to individual program participants. This information could be found in participant files and

data sets, performance reports, program evaluations, grant and contract files, and other sources.

The WDB expects all staff and representatives to respect the privacy of clients and to maintain their personal and financial information as confidential. Access to any PII must be restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to the scope of work in the grant or contract agreement. No information may be released without appropriate authorization.

CUSTOMER AWARENESS

Individuals must be informed in writing how their information will be used and that their information will be protected and that their personal and confidential information:

- May be shared among federal and state agencies, partner staff and contractors;
- Is used only for delivering services and that further disclosure of their confidential information is prohibited; and that
- PII will be used for grant and eligibility purposes only.

Every individual receiving WIOA or other WDB services must read, sign and date a Release of Information to share their information with partner agencies. Individuals must be informed that they can request that their information not be shared among partner agencies and that this does not affect their eligibility for services.

Staff and representatives should engage in practical ways to reduce potential security breaches and protect sensitive information and PII by:

- Reducing the volume of collected and retained information to the minimum necessary;
- Limiting access to only those individuals who must have such access; and
- Using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

PROTECTING INFORMATION

PII and confidentiality require special precautions to protect them from unauthorized use, access, disclosure, modification, and destruction. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Staff will exercise extreme care and caution when working with confidential information to ensure the privacy of the applicant or customer.

Physical Data Protection Requirements

All sensitive or PII data obtained should be stored in an area that is physically safe from access by unauthorized persons at all times. Staff and representatives must not leave personal and confidential information left open and unattended.

When a staff or representative's desk is unattended, it is the staff or representative's responsibility to ensure that personal and confidential information, including PII, is

secured in closed containers such as locked drawers or offices when not in use. This means that all documents containing personal and confidential information must not be left on desks, fax machines, printers, or photocopiers unattended. Desktops and computers will be kept clear of papers and/or files containing confidential information that are not being used. Desktops and computers will be kept clear of confidential information during non-business hours.

Any papers containing PII and/or confidential information are to remain in the offices of the WDB, except invoices may be transported directly to the County accounting offices, and, upon occasion, there may be other papers that must be transported to other locations for a specific purpose and with the express permission of the Unit Manager. All discarded paper containing confidential information shall be placed in a locked shredder bin or shredded.

Any participant files stored for performance or archiving purposes must be clearly marked as containing personal and confidential information. Staff and representatives should retain participant PII only for the period required for assessment or performance purposes. Thereafter, all data must be destroyed by a qualified company to minimize risk of breach.

Electronic Data Protection Requirements

To safeguard WDB's electronically stored data, each user will receive a designated and authorized log-on(s) and password(s) that restrict users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. This is such that unauthorized persons cannot reasonably retrieve the information by means of a computer.

The WDB expects all staff to secure mobile equipment, such as laptop computers and other devices that may have PII stored on them. Devices should be password protected and safeguarded when not in use. Accessing and storing data containing PII on personally owned equipment at off-site locations, such as the employee's home, and on non-managed IT services, such as Google or Yahoo, is prohibited.

TRANSMISSION OF CONFIDENTIAL INFORMATION

Staff and representatives should avoid communicating sensitive information or PII about an applicant or participant to partner agencies or other staff via email. If it is necessary, staff and representatives must ensure that the intended recipient is the only individual that has access to the information and that the recipient understands they must also protect the information. Staff and representatives must only communicate sensitive information or PII through WDB emails and not through third party or personal email addresses.

PII and other sensitive data transmitted via email or stored on mobile data storage (such as thumb drives) must be encrypted. Staff and representatives must not e-mail unencrypted sensitive PII to any entity, including the Department of Labor, WDB staff, or

contractors. Staff and representatives should discourage participants from emailing personal and confidential information to their case managers.

Any information posted to social media sites is considered public record and is subject to public disclosure. No sensitive information or PII should be posted to social media sites.

Care shall also be taken to ensure that unauthorized individuals do not overhear any discussion of confidential information.

SOCIAL SECURITY NUMBERS

Social security numbers are protected as high-risk information. When requesting a participant's social security number, staff and representatives should explain how the social security number will be used and how the participant's privacy will be ensured.

Staff must request a participant's social security number when offering the following services:

- Staff-assisted service related to eligibility determination, job search activity, and employment;
- All training and educational services; and
- Self-services through CalJOBS.

However, an individual is not required to provide their social security number to receive WIOA services, and services cannot be denied to an individual due to their refusal to disclose their social security number.

Whenever possible, staff and representatives should use unique identifiers for participant tracking instead of social security numbers. While social security numbers may be needed for initial eligibility or performance purposes, a unique identifier should be linked to each individual record and used thereafter. This includes such records as training or contract documents. If social security numbers are to be used for specific tracking purposes, they must be stored or used in such a way that it is not attributable to the individual. For example, a training document should not include the participant name and social security number, rather the participant name and a truncated social security number.

Social Security numbers may not be listed on anything mailed to a client or to another agency unless required by law, or the document is a form or application. Social Security numbers may not be left on a voice mail message.

MEDICAL AND DISABILITY RECORDS

Medical and disability records are additionally protected as confidential information. To ensure the information is protected, any medical or disability records must be kept separately from working participant files and kept in a secured physical and/or electronic location. Only the portion of the participant's information that reveals the presence of a

disability or other data element should be included in the participant's file to minimize staff and representative access to medical files.

Once collected, access to the medical file should be limited and only accessed:

- With the approval of program management and only when necessary for WIOA service delivery;
- By first aid and safety personnel in the event of an emergency; or
- By local, state, or federal monitors.

When all WIOA or other WDB services are complete and the participant file is ready to be archived, participant medical and disability-related information must be placed in a sealed envelope and marked "Medical and Disability Information."

SECURITY BREACHES

Any staff or representative who becomes aware of any actual or attempted PII security breach resulting from the inadvertent or intentional leak of release of confidential information, including PII, shall immediately inform their direct supervisor. PII security incidents include, but are not limited to, any event (intentional or unintentional) that causes the loss, damage, or destruction, or unauthorized access, use, modification, or disclosure of information assets. The system or device affected by a PII security incident shall be immediately removed from operation. It shall remain removed from operation until correction and mitigation measures are applied.

Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach. Supervisors should bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

Four factors should be considered to assess the likely risk of harm:

- Nature of the Data Elements Breached
- Number of Individuals Affected
- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm

WDB will inform the California Employment Development Department of breaches believed to cause harm. Breaches subject to notification requirements include both electronic systems as well as paper documents.

Individuals assessing the likely risk of harm due to a security breach should exercise the objectivity principle, which requires individuals to show the highest professional objectivity level in collecting, assessing, and communicating information about the breach examined. Further, assessors are expected to perform a balanced assessment of every relevant situation and they must not be influenced by their own or other people's interest while forming judgments.

STAFF COMPLIANCE

All WDB employees with access to participant PII and/or confidential information must sign an acknowledgement that they have read the policy, understand the confidential nature of participant data and the potential sanctions for improper disclosure, and agree to abide by all other requirements and terms contained therein.

Unauthorized disclosure of confidential or privileged information is a serious violation of this policy. Any failure to comply with confidentiality requirements identified in this policy may result in termination or suspension of contract or employment, or the imposition of special conditions or restrictions to protect the privacy of participants or the integrity of PII data. Misuse or noncompliance with PII data safeguards could lead to civil and criminal sanctions per federal and state laws.

Staff and representatives are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service.

DISCLAIMER

This policy is based on WDB's interpretation of the statute, along with the Workforce Innovation and Opportunity Act; Final Rule released by the U.S. Department of Labor, and federal and state policies relating to WIOA implementation. This policy will be reviewed and updated based on any additional federal or state guidance.

REFERENCES

Law

- Workforce Innovation and Opportunity Act of 2014 (WIOA)
- Privacy Act of 1974, Section 7
- California SB168, Title 1.81.1 – Confidentiality of Social Security Numbers
- California AB763 – Privacy: Social Security Numbers
- Federal Information Security Management Act (FISMA)

Federal Guidance

- Training and Employment Guidance Letter (TEGL) 05-08 – Policy for collection and Use of Workforce System Participants' Social Security Numbers
- TEGL 39-11 – Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- OMB Memorandum M-07-16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- NIST SP 800-122 – Guide to Protecting the Confidentiality of PII

Approved by

Workforce Development Board of Solano County

ATTACHMENT A: Staff/Representative Confidentiality Agreement

WORKFORCE DEVELOPMENT BOARD
OF SOLANO COUNTY

STAFF/REPRESENTATIVE CONFIDENTIALITY AGREEMENT

I, _____ [print name] certify that I have read and understand the Workforce Development Board of Solano County's (WDB) policy on **USE AND CONFIDENTIALITY OF PARTICIPANTS' PERSONALLY IDENTIFIABLE INFORMATION (PII)**. I understand that I may have access to customer and employer confidential records as part of my employment, contracting, or volunteer work with the WDB. Confidential information provided to our agency by any participant or by any federal, state, or county entity is protected by law, regulation, and policy.

I understand that it is my responsibility as part of the workforce development system in Solano County to protect the confidentiality of all Workforce Innovation and Opportunity Act (WIOA) applicants and participants, as well as customers utilizing the Solano Employment Connection, an affiliate of the America's Job Centers of California (AJCC) system. I understand that in the workforce system's collection, usage, storage and transmission of customer information, the tenets of confidentiality are to be strictly enforced.

I understand that I have the responsibility to know whether information is protected. If I have any questions regarding whether particular information is confidential, I understand it is my responsibility to check with my supervisor.

I understand that unauthorized access, use, modification, or disclosure of confidential information is a crime under state and federal laws, including but not limited to California Information Privacy Act §1798.53-§1798.57, CA Penal Code §502, §2111 of the Unemployment Insurance Code, and §10850 of the Welfare and Institutions Code. I understand that violation of this policy could result in:

- Disciplinary action
- Termination of employment
- Criminal action (including incarceration)
- Civil action

By signing below, I agree to follow and be bound by the terms and conditions regarding confidentiality of personal information contained therein. WDB staff or their designee have answered any questions I may have had regarding this policy.

Signature:_____

Name:_____ Date: _____

ATTACHMENT B: Participant Confidentiality Rights

WORKFORCE DEVELOPMENT BOARD
OF SOLANO COUNTY

PARTICIPANT CONFIDENTIALITY RIGHTS

Your privacy is one of our primary concerns. The Workforce Development Board of Solano County (WDB) makes every effort to provide you with a safe and private environment. The information below explains what information we gather and how we use it. It applies to all WDB uses of information and is intended to protect the confidentiality of all customer information.

Access to Data
Program staff must collect data in order to document eligibility and provide services per federal regulation under the Workforce Innovation and Opportunity Act (WIOA). The WDB and subcontractors will make every effort to collect and store data in a secure manner. Access to any personal customer information is restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to service delivery.

For auditing and monitoring purposes, individuals' personal and confidential information may be shared among federal and state agencies, partner staff and contractors under the WDB umbrella. Access is for the purpose of determining compliance with, and ensuring enforcement of the provisions of WIOA.

Use and Release of Data
We may ask you to provide personal information when you:

- Use the CalJOBS website;
- Request services, support or information to validate eligibility;
- Share WDB content through social media;
- Subscribe to newsletters, or other materials; or
- Contact us for information on services available.

Information we may request includes your email address, name, address, telephone number, proof of U.S. residence, proof of age, selective service verification, and other data elements depending on program eligibility criteria. Data will only be used for the purposes of verifying eligibility, delivering services, and verifying performance measures. Upon request, data can be released to the subject of the information.

You may decide whether or not to provide your social security number. If you do not wish to provide this number, you can still receive services. The authority for the solicitation of social security numbers is from the California Unemployment Insurance Code, Section 15026. If you choose to provide your number, these are the ways it may be used by the WDB or the State of Studies and evaluation of training and employment programs in which you may participate:

- Getting information for future program and budget planning;
- Checking for possible participation by you in other state or federal programs;
- Studying long-term effects on all participants in this program;
- Finding ways to make this program more effective; or
- Sharing information with other employment and training programs.

ATTACHMENT B: Participant Confidentiality Rights

How We Protect Your Data
To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards, secured files, and secured buildings. All sensitive individual data is stored in an area that is physically safe from access by unauthorized persons at all times and data transmitted electronically is encrypted.

Medical and disability records are additionally protected as confidential information. Any medical or disability records are kept separately in a secured physical and/or electronic location. Social security numbers are also protected as high-risk information. Whenever possible, staff and representatives will use unique identifiers to track individual data rather than personally identifiable information.

Disclosing Personal Information
The WDB may share your Personal Information with California Employment Development Department and U.S. Department of Labor monitors for the purpose of assessing programmatic and fiscal compliance. In addition, we may disclose your personal information when legally required or to protect our rights. Any other use of individual data will require written consent from the customer or customer's parent/legal guardian.

Notification of Privacy Changes
The WDB privacy rights are outlined in the Use and Confidentiality of Participants' Personally Identifiable Information (PII) policy which can be found on the WDB's website at: http://www.solanoemployment.org/wioa-policies. The WDB reserves the right to make changes to this policy at any time. When changes are made they will be posted and available immediately with a revised effective date. We encourage you to periodically review the privacy policy.

Acknowledgement of Receipt

By signing below, I acknowledge that I have explained this agreement to the WDB-affiliated customer.

Staff Printed Name: _____

Staff Signature: _____ Date _____

By signing below, I acknowledge that I have read and understand this agreement. WDB staff have explained this agreement and answered any questions I may have had.

Individual Printed Name: _____

Individual Signature: _____ Date _____

(Parent / Guardian Name and Signature if under 18 years of age)

Definitions of Key Terms

Personally Identifiable Information (PII) as defined by OMB Memorandum M-07-16 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal information that is linked or linkable to a specific individual.

There are two types of PII as defined by the U.S. Department of Labor in TEGL 39-11 that are based on the "risk of harm" that could result from the release of the PII:

- Protected PII – is any information that if disclosed could result in harm to the individual whose name or identify is linked to that information. Examples include, but are not limited to, social security numbers, credit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometrics identifiers, medical history, financial information, and computer passwords.
- Non-Sensitive PII – is information that if disclosed, by itself, could not reasonably be expected to result in personal harm as it is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

A combination of non-sensitive PII could potentially be categorized as protected PII. As example, a name and business e-mail address will not result in a high degree of harm to an individual. A name linked to a social security number and date of birth could result in identity theft.

A **Security Breach** as defined by TEGL 39-11 is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Sensitive Information as defined by TEGL 39-11 is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest of the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.