Attachment A

INFORMATION RELEASE CONTRACT BETWEEN TEXAS WORKFORCE COMMISSION AND COLLIN COUNTY FBO DISTRICT ATTORNEY'S OFFICE

STATEMENT OF WORK – PROJECT OBLIGATIONS

SECTION 1 – Project Abstract

1.1 Contract Purpose. The purpose of this Contract is to provide Recipient with access to confidential Agency data, to ensure that Recipient will maintain the confidentiality of the data, and to require Recipient to reimburse Agency for costs of providing access at the rates set out in this Contract.

1.2 Authorized Use of TWC Information. Subject to the security and confidentiality provisions of this Contract, Recipient is authorized to use TWC Information, as defined in Attachment B, item 1, solely for the Limited Purpose(s) listed in the Request and Safeguard Plan and associated correspondence which is incorporated into this Contract and marked as Exhibit 1. Recipient warrants that all statements and information in Exhibit 1, Request and Safeguard Plan and associated correspondence true and correct to the best of my knowledge and understands that their organization is bound by the representations in Exhibit 1. Any other use of TWC Information by Recipient is a breach of this Contract.

1.3 References. Section references are to sections of this Attachment A unless otherwise specified.

SECTION 2 – Obligations of Agency

2.1 Description of TWC Information Disclosed and Method of Access. Agency agrees to provide access to the TWC information requested and via the method as described in Exhibit 1.

2.2 Availability. Online access will routinely be available Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time, excluding State holidays, although Agency does not guarantee access during these periods. Agency may terminate or limit access without notice based on business necessity or in the event of an emergency.

2.3 Method of transfer. Agency will transfer TWC Information to Recipient only as specified in the Request and Safeguard Plan or by other methods approved in writing in advance by Agency Chief Information Security Officer or his/her designee.

SECTION 3 – Obligations of Recipient

3.1 Online Access.

3.1.1 Direct Oversight of Users. Recipient shall ensure that all individuals with online access through user TWC system log-in accounts ("Users,") are direct Recipient employees.

3.1.2 Annual Fee and Payment. Recipient shall pay Agency the annual subscription fee applicable to the access identified in Exhibit 1, Request and Safeguard Plan. The annual subscription fee covers the twelve (12) month period that begins on the Begin Date. Payment of the annual subscription fee is due within thirty (30) calendar days of Recipient's execution of this Contract. The annual subscription fee is nonrefundable and will not be prorated in case of early termination of this Contract or suspension of services. If access identified in the Request and Safeguard Plan in Exhibit 1 is for multiple years, the Recipient shall pay Agency the annual subscription fee for each subsequent contract year within thirty (30) calendar days of the beginning of each contract year. If the contracting entity is a city or county, also known as a "local entity", Recipient shall send payment to Texas Workforce Commission, Revenue and Trust Management, P.O. Box 322, Austin, TX 78767-0322.

3.1.3 User Documents. All prospective online Users must execute a Texas Workforce Commission User Agreement ("User Agreement"), Attachment C, and complete online TWC Cybersecurity Awareness Training ("Security Training").

3.1.4 User Document Submission and Maintenance. Before Agency EAGLE Administration will invite a prospective User, Agency EAGLE Administration must receive from Recipient Contact Person (designated in Exhibit 1, Request and Safeguard Plan) a copy of the completed Texas Workforce Commission User Agreement ("User Agreement"), Attachment C and the Security Training certificate with a completed Transmittal Cover Sheet ("Cover Sheet"), Attachment D. Agency may deny access to any prospective User on security grounds. Recipient must maintain on file all original Training Certificates and User Agreements, which are subject to on-site and desk review audits.

3.1.5 Annual User Renewal. For multi-year, extended, and new contracts continuing, extending, or replacing a prior contract with online access, each year, on the first day of the month following the anniversary of the Begin Date the Recipient Contact Person shall provide new User Agreements and the Security Training certificate. The User Agreements and Security Training certificates shall be submitted with a completed Cover Sheet no earlier than 30 days before the first day following the anniversary of the Begin Date. The User Agreements and Training Certificates shall be executed and dated no more than thirty (30) calendar days before submission. Failure by Recipient Contact Person to timely provide annual User Agreements, shall result in Agency terminating User access.

3.1.6 Notice of User Employment Change. Recipient Contact Person shall notify Agency EAGLE Administration within three (3) calendar days of a User's termination, resignation, or reassignment into a position not requiring access to TWC Information, so that the User's password can be immediately revoked. Failure to provide such notice is a breach of this Contract and may result in immediate suspension of all online access, termination of this Contract, and other penalties provided by law and this Contract.

3.1.7 Monthly Review. For contracts with over twenty-five (25 users), Recipient Contact Person shall review the list of current Users monthly to ensure that the Users have not left employment or changed job duties or otherwise no longer need access. Recipient shall document their process for comparing the current users list with the list of employees needing access. The

documentation of the review process should be maintained on file for review by Agency upon request.

3.1.8 Notice of Suspected Violations. Recipient shall notify Agency of any suspected or confirmed User violation of the confidentiality and security provisions within twenty-four (24) hours of discovery and shall take appropriate corrective action.

3.1.9 Changes to TWC Information Prohibited. Users shall not change or update any TWC Information contained in Agency's computer stored files. Users shall not use any automated system or software to make multiple queries of Agency's computer stored files.

3.1.10 Instructions. Recipient shall be solely responsible for disseminating to Users any instructions provided by Agency regarding navigation of online access to TWC Information.

3.2 Offline Access. If Offline access is selected in Exhibit 1, Request and Safeguard Plan, the provisions of this section apply.

3.2.1 Offline Request Submission. For matches of wage records to SSNs, unemployment compensation claim benefit data to SSNs, or employer tax records to EIDs or FEINs, to be performed by Agency staff, Recipient shall submit a completed *Request for Texas Workforce Commission Records*, Attachment E, with the file of SSNs, EIDs, or FEINs to be matched. Recipient shall submit the file electronically in compliance with the Information Technology Department contract listed on Exhibit 1, Request and Safeguard Plan. Agency shall not be responsible for the confidentiality of any information submitted by Recipient.

3.2.2 Offline Rates. Rates for Offline requests are calculated on a per-request basis as specified in Exhibit 1, Request and Safeguard Plan.

3.2.3 Payment. Recipient's payment is due within thirty (30) calendar days of receipt of invoice for information requested Offline.

3.2.4. Tracking of Offline Access. Each quarter, the Recipient shall submit to the Agency Point of Contact a list of the data requests made and data received during the prior quarter including information necessary for identifying each transfer of data, whether a match against Recipient data, a scheduled transfer, or a transfer upon request. The quarterly filing dates are January 15, April 15, July 15, and October 15.

3.3 Additional Requirements.

3.3.1 Security Safeguards. Recipient shall establish, maintain, and comply with security safeguards and procedures to protect the confidentiality of all TWC Information. Recipient shall comply with the requirements in *Safeguards for TWC Information*, Attachment B. Failure to comply with any requirement of Attachment B is a breach of this Contract.

3.3.2 Suspension. Agency may suspend all services without notice if Agency suspects a violation of the security safeguard provisions in Attachment B. Services will remain suspended until Agency has fully investigated any suspected security violations and is satisfied that resumption of services will not result in security breaches. In the event of an extended suspension of services, Agency will notify Recipient as soon as possible.

3.3.3 Enduring Obligation. Termination or expiration of this Contract will not end Recipient's responsibility to protect the confidentiality of TWC Information remaining in Recipient's possession, under Recipient's control, or held by a third party subject to contract or agreement with Recipient.

3.3.4 Audit. Recipient's security safeguards and procedures, as well as Recipient's access to and use of TWC Information, are subject to monitoring, evaluation, and audit by Agency.

3.3.5 Inspections. Recipient shall cooperate fully with any on-site inspections and monitoring activities of Agency. So that Agency may audit Recipient's compliance with the requirements of state and federal law and this Contract, Recipient shall permit Agency access to all sites containing TWC Information (including sites where data is maintained electronically), and to all workplaces used by personnel who have access to TWC Information.

3.3.6 Self-Assessment Report. Recipient shall submit to Agency a fully executed *Quarterly Self-Assessment Report*, Attachment G, on the next-occurring quarterly filing date after the Begin Date, and on each quarterly filing date for as long as this Contract is in effect. The quarterly filing dates are January 15, April 15, July 15, and October 15. Each report must be completed after the end of the prior calendar quarter and must have been signed within fifteen (15) days preceding submission. Failure by Recipient to submit to Agency a timely Quarterly Self-Assessment Report may result in the following consequences: the first instance of a late Quarterly Self-Assessment Report shall result in a late notice being issued by TWC. A failure by Recipient to timely respond to the first late notice by the time specified in the notice or Recipient receiving a second late notice, may result in TWC terminating the Contract for cause.

3.3.7 Identity Theft Protection. In case of unauthorized disclosure of TWC Information by Recipient, Recipient shall purchase identity theft protection service for all individuals whose information was disclosed without authorization. The protection service shall cover each individual for a two-year period and must include, at a minimum, automatic fraud alerts to the individual.

3.3.8 Significant Change. Recipient agrees to notify Agency in writing within ten (10) calendar days of any significant change affecting Recipient and Recipient's identity, including but not limited to changes in its ownership or control, name, governing board membership, authority of governing board, officeholders, or vendor identification number.

3.3.9 Computer Resources. Recipient shall provide and maintain its own computer hardware and software to accomplish the necessary computer communications linkages with Agency.

3.3.10 Data Source. Agency does not warrant or guarantee the accuracy of TWC Information. TWC Information includes data provided to Agency by third parties, including employers and employees.

SECTION 4 – Contact Persons

4.1 Designation. The Parties designate the primary liaisons as specified in Exhibit 1. Request and Safeguard Plan.

Agency Contact Person

Contract Management Team
External Data Exchange Contracts (EDE)
Procurement and Contract Services Department
Texas Workforce Commission
1117 Trinity Street, Room 342T
Austin, TX 78701

Phone: (737) 400-5482
Fax: (512) 936-0219
Email: DEContracts@twc.texas.gov

4.2 Notice. Any notice required under this Contract must be given to the Recipient's Contact Person specified in Exhibit 1. Request and Safeguard Plan or the Agency Contract Person.

4.3 Notice to Alternate. If Recipient designates an alternate Contact Person in Exhibit 1, Request and Safeguard Plan, written notification by Agency to one (1) of the Recipient Contact Persons will satisfy any notification requirement of this Contract.

4.4 Change. Recipient may request a change in Recipient Contact Person by submitting to Agency Contact Person a written request on organizational letterhead signed by the person who signed this Contract on behalf of Recipient, or by a successor with authority to bind Recipient contractually. The request must include the TWC Contract Number, the name of the person being replaced, and the name of the new Recipient Contact Person, with job title, work address, phone number, and email address. No change in Recipient Contact Person is effective until acknowledged in writing by Agency.

4.5 Communications. Recipient shall include the TWC Contract Number in all communications with Agency.

SECTION 5 – Parties Option for Extension and Effect on Other Contracts

The Parties agree that this Contract supersedes and replaces all prior contracts, if any, between them for information release or data sharing as specified in Exhibit 1. Request and Safeguard Plan.

In the event contract renewal negotiations are not completed prior to the contract expiration date, both parties agree that services shall be provided by the Agency and accepted by Recipient, subject to all original terms and conditions of the contract, for a period not to exceed ninety (90) days following the original contract expiration date. During the holdover extension period, costs shall remain at the rate in effect immediately prior to expiration of the original contract period and all other terms and conditions shall remain in effect.

(Use only for external EAGLE Administrators with over 100 Users)
SECTION 6 – Recipient EAGLE Administrator Role and Responsibilities

6.1 Recipient's EAGLE Administrator. In addition to the procedures described in Section 3.1.3 regarding Agency's grant of online access, Agency may enable a **maximum of _____ ( ) Recipient employee(s) as EAGLE Administrator(s)** to administer access on Agency's computer system for individuals selected as Users by Recipient. All Users must be direct Recipient employees. Administration of User access includes, among other things, issuance of User IDs and passwords,

terminating User access, reviewing current User access and EAGLE reports, addressing User access violations, and submitting required reports to Agency.

6.2 Designation and Training. Recipient shall designate an initial EAGLE Administrator and any subsequent EAGLE Administrators in writing to Agency Contact Person. All designated EAGLE Administrators must execute a User Agreement, complete Agency Cybersecurity Training, and review the online Agency EAGLE User Guide. To access the EAGLE User Guide, open EAGLE and click on the EAGLE User Guide at the top right corner of the page.

6.3 Maximum Number of Users. The maximum number of Users specified in Section 2.1.2 includes Users granted access by Agency EAGLE Administration and Users granted access by Recipient's EAGLE Administrator. Allowing users to create an EAGLE account by Recipient's EAGLE Administrator such that this combined number exceeds the maximum number of Users is a breach of this Contract and may result in termination of EAGLE Administrator authorization as well as imposition of the penalties listed in Section 6 of the General Terms and Conditions. The maximum number of Users may be modified only by contract amendment.

6.4 Screening. Recipient's EAGLE Administrator shall screen potential Users and issue User IDs and passwords only to employees that EAGLE Administrator has determined pose no threat to the security of TWC Information.

6.5 User Documents. Recipient's EAGLE Administrator shall obtain a completed User Agreement and a Training Certificate from each User before allowing the User to register for online access and shall keep the original Training Certificates on file.

6.6 Authorization. Agency authorizes Users who have been assigned User IDs and passwords by the EAGLE Administrator to access the screens listed in Section 2.1.1, for the Limited Purpose in Section 1.2 only.

(Use this section only for renewing contracts.)

6.7 User Document Renewal. **On _____ (insert date one month after Begin Date)** EAGLE Administrator shall terminate the online access of each User established under a prior contract unless before that date EAGLE Administrator receives a new User Agreement and new Training Certificate for the User executed or dated, respectively, no more than thirty (30) calendar days before submission. EAGLE Administrator must obtain and maintain Training Certificates and User Agreements for all Users to whom User IDs have been issued. EAGLE Administrator shall immediately delete a User's ID upon termination of the User's employment with Recipient or reassignment to a position not requiring access to TWC Information.

(Use this section only for renewing contracts.)

6.8 Manager Document Renewal. **On _____ (insert date one month after Begin Date)** each EAGLE Administrator accessing the system under a prior contract will be denied access to the system unless before that date Agency EAGLE Administration has received for the EAGLE Administrator, from Recipient Contact Person, copies of a new User Agreement and new Training Certificate executed or dated, respectively, no more than thirty (30) calendar days before submission, with a completed Cover Sheet, Attachment D.

Use this section only for contracts longer than one year.)

6.9 Annual User Renewal. On each anniversary of the Begin Date, EAGLE Administrator shall terminate access of any User for whom EAGLE Administrator does not have on file a User Agreement and a Training Certificate executed or dated, respectively, no more than thirty (30) calendar days before the anniversary.

Use this section only for contracts longer than one year.)

6.10 Annual Manager Renewal. On each anniversary of the Begin Date, each EAGLE Administrator will be denied access to the system unless before that date Agency EAGLE Administration has received for the EAGLE Administrator, from Recipient Contact Person, copies of a new User Agreement and new Training Certificate executed or dated, respectively, no more than thirty (30) calendar days before submission, with a completed Cover Sheet, Attachment D.

6.11 Monthly Report. EAGLE Administrator shall provide to Agency a written report within fifteen (15) calendar days after the end of each month, listing all Users authorized for online access at any time during the previous month, with their work addresses. EAGLE Administrator shall provide a list of the names, and work addresses of all current Users, and copies of their User Agreements and Training Certificates, at any time upon Agency request.

6.12 Annual Report. Within thirty (30) calendar days after each anniversary of the Begin Date, EAGLE Administrator shall submit to Agency a list of current Users for whom EAGLE Administrator has on file a User Agreement and a Training Certificate for the User executed or dated, respectively, no more than thirty (30) calendar days before the anniversary. Agency will revoke access of any User not included on the list.

6.13 Training Dissemination. Following Agency's training of the originally-designated EAGLE Administrator to access TWC Information, EAGLE Administrator will be solely responsible for disseminating such training to additional EAGLE Administrators.

6.14 Responsibility. Recipient shall be responsible for ensuring that each EAGLE Administrator complies with the provisions of this Contract and shall be liable and responsible for all actions of each EAGLE Administrator.

(Use only for authorized re-disclosure under Section 11.3 of Attachment B and renumber accordingly.)

SECTION 7 – Re-Disclosure Authorization, Roles and Responsibilities

7.1 Re-disclosure Authorization. Notwithstanding the provisions set forth in Sections 10 and 11 regarding unauthorized and authorized redisclosure, Recipient is authorized to re-disclosure TWC Information for the Limited Purposes specified in Exhibit 1, Request and Safeguard Plan, consistent with 20 CFR § 603.9(c)(1)(v), to Recipient's agent or contractor, provided Recipient retains responsibility for the uses of the confidential TWC Information by Recipient's agent or contractor and complies with the safeguards in Attachment B, Safeguards for TWC Information, to the same extent and degree as those safeguards are applicable to Recipient's use of TWC Information.

7.2 Re-disclosure Additional Safeguards. For Recipient's re-disclosure of any TWC information permitted under this Section 6 of Attachment A, Recipient shall be responsive for all re-disclosure by their contractor or agency.

7.3 Re-disclosure Audit. If re-disclosure is approved, Recipient's security safeguards and procedures, as well as Recipient's access to, use of and re-disclosure under Attachment B, Section 11.3, of TWC information, are subject to monitoring, evaluation, and audit by Agency.

7.4 Re-disclosure Identity Theft Protection. If re-disclosure is approved in Attachment B, Section 11.3, Recipient shall purchase identity theft protection service for all individuals whose information was disclosed without authorization by any entity provided information by Recipient under Section 11.3 of Attachment B. The protection service shall cover each individual for a two-year period and must include, at a minimum, automatic fraud alerts to the individual.

Attachment B

SAFEGUARDS FOR TWC INFORMATION

1. "Recipient" in this Contract shall maintain sufficient safeguards over all TWC Information to prevent unauthorized access to or disclosure of TWC Information:

   "TWC Information" means records maintained by Agency (TWC), and records obtained by Recipient from Agency under this Contract, including (1) records and data compilations provided electronically, on paper, or via online access or e-mail, (2) records and data compilations that Recipient has converted into another format or medium (such as handwritten or electronic notes), and (3) records and data compilations incorporated in any manner into Recipient's records, files, or data compilations.

2. Monitoring. Recipient shall monitor its Users' access to and use of TWC Information and shall ensure that TWC Information is used only for the following "Limited Purpose" as set forth in Exhibit 1, Request and Safeguard Plan. Recipient shall also ensure that TWC Information is used only for purposes authorized by law and in compliance with all other provisions of this Contract.

3. Storage. Recipient shall store TWC Information in a place physically secure from access by unauthorized persons.

4. Protection. Recipient shall store and process TWC Information, including that maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain TWC Information by any means.

5. Access. Recipient shall undertake precautions to ensure that only authorized personnel are given access to TWC Information stored in computer systems.

6. Instruction. Recipient shall instruct all personnel having access to TWC Information about all confidentiality requirements including the requirements of 20 C.F.R. Part 603 as well as the sanctions specified in this Contract and under state and federal law for unauthorized disclosure of TWC Information. Recipient acknowledges that all personnel who will have access to TWC Information have been instructed as required.

7. Disposal. Recipient shall dispose of TWC Information and any copies thereof after the Limited Purpose(s) is achieved, except for TWC Information possessed by any court. Disposal means return of TWC Information to Agency or destruction of TWC Information, as directed by Agency. Disposal includes deletion of personal identifiers in lieu of destruction. In any case, Recipient shall dispose of all TWC Information within thirty (30) calendar days after the termination, cancellation, or expiration of this Contract, in accordance with Attachment F, *Certificate of Destruction for Contractors and Vendors,* which is attached to this Contract and incorporated for all purposes.

8. System. Recipient shall establish and maintain a system sufficient to allow an audit of compliance with the requirements of this Attachment B and the other provisions of this Contract.

9. No Disclosure or Release. Recipient shall not disclose or release any TWC Information other than as permitted in this Contract, without prior written consent of Agency.

10. Unauthorized Disclosure. It is a breach of this Contract to disclose TWC Information orally, electronically, in written or printed form, or in any other manner without the prior written consent of Agency:
    10.1 to any contract employee of Recipient or any individual not employed by Recipient;

    10.2 to another government entity, including a law enforcement entity;

    10.3 to Recipient employees who do not have a need to use TWC Information for the Limited Purpose.

11. Authorized Disclosure. TWC Information may only be disclosed:
    11.1 to employees under the direct hiring-and-firing control of Recipient who have a need to use the TWC Information for the Limited Purpose(s); and

    11.2 in a criminal judicial proceeding if the TWC Information is introduced in court as a sealed record with access limited to the prosecutor, defendant, judge, and jury.

    11.3 (Add 11.3 if Agency is authorized to re-disclose with other entities)

12. Security Violation. Recipient shall monitor access of Users and shall notify Agency within twenty-four (24) hours if a security violation of this Contract is detected, or if Recipient suspects that the security or integrity of TWC Information has or may have been compromised in any way.

13. Format. TWC Information is subject to the requirements of this Contract even if the TWC Information is converted by Recipient into another format or medium, or incorporated in any manner into Recipient's records, files, or data compilations.

14. Access Limited. Recipient shall limit access to TWC Information to its employees who need access to achieve the Limited Purpose.

15. Mobile Device and Removal. Recipient shall not place TWC Information on mobile, remote, or portable storage devices, or remove storage media from Recipient's facility, without the prior written authorization of Agency.

16. Public Information Act. Under Texas Labor Code § 301.085, TWC Information is not "public information" for purposes of the Public Information Act, Texas Government Code, Chapter 552. Recipient shall not release any TWC Information in response to a request made under the Public Information Act or under any other law, regulation, or ordinance addressing public access to government records.

17. Subpoena. Recipient shall notify Agency within twenty-four (24) hours of the receipt of any subpoena, other judicial request, or request for appearance for testimony upon any matter concerning TWC Information. Federal regulations dictate the handling of subpoenas for TWC Information. Recipient shall comply with the requirements of 20 C.F.R. § 603.7 in responding to any subpoena, other judicial request, or request for appearance for testimony upon any matter concerning TWC Information.

18. Federal Regulation. Recipient shall comply with all requirements of *Safeguards for TWC Information* ***as required by 20 CFR Part 603 and*** this Contract relating to safeguarding TWC Information and ensuring its confidentiality.

19. Unauthorized Lookup. A User shall not access TWC Information listed under the User's SSN or the SSN of a co-worker, family member, or friend.

20. Screening – Online Users. Recipient shall screen potential Users and seek online access only for employees that Recipient has determined pose no threat to the security of TWC Information.

21. Screening – All Handlers. Recipient shall permit access to TWC Information only to employees that Recipient has determined pose no threat to the security of TWC Information.

22. Internet. Recipient shall not transmit any TWC Information over the Internet unless it is encrypted using at least 256-bit AES encryption and the current FIPS 140 series encryption standards.

23. Screen Dump. Recipient's security guidelines shall ensure that any screen dump or other extraction of TWC Information will be protected from unauthorized use or disclosure.

24. No Transfer. Recipient shall not transfer the authority or ability to access or maintain TWC Information under this Contract to any other person or entity.

(Add if re-disclosure approved as provided in Section 11.3, of Attachment B.)

25. Additional Re-Disclosure Authorization, Roles and Responsibilities. Notwithstanding Sections 10 and 11 of this Attachment B, Safeguards for TWC Information, Recipient is authorized to re-disclose TWC Information for the Limited Purposes specified in Exhibit 1, Request and Safeguard Plan, consistent with 20 CFR § 603.9(c)(1)(v), to Recipient's agent or contractor, provided Recipient retains responsibility for the uses of the confidential TWC Information by the agent or contractor and complies with the following additional safeguard provisions in this section 25.

25.1 Additional Re-Disclosure Safeguard Standards. Recipient shall hold Contract personnel to the same standard of processing, training, and protecting information as Recipient employees who have a need to use the TWC information for the Limited Purpose.

25.2 Additional Re-Disclosure Monitoring Requirements. Recipient shall monitor its Users' access to and use of TWC *as well as the access to and use of TWC Information by those contractors or agents to which TWC Information has been redisclosed under this Section 25* and shall ensure that TWC Information is used only for the "Limited Purpose(s)" set forth in **Exhibit 1, Request and Safeguard Plan.** Recipient shall also ensure that TWC Information is used only for purposes authorized by law and in compliance with all other provisions of this Contract.

25.3. Additional Instruction for Re-Disclosure: Recipient shall instruct *each entity to which TWC Information has been re-disclosed under this Section 25* about all confidentiality requirements including the requirements of 20 C.F.R. Part 603 as well as the sanctions specified in this Contract and under state and federal law for unauthorized disclosure of TWC Information. Recipient acknowledges that each entity has been so instructed as required.

25.4. Additional Disposal Requirements for Re-Disclosure. For any TWC Information re-disclosed under this section 25, Recipient shall require as a condition of re-disclosure that any federal agency to which TWC Information has been re-disclosed agree to no further disclosure of TWC Information and to return such TWC Information to Recipient when no longer needed or to confirm that the information has been properly destroyed by shredding or burning.

Remainder of page intentionally left blank.

(Keep only for PENs and PEBs, and NFAs with online access) **Attachment C**

TEXAS WORKFORCE COMMISSION USER AGREEMENT

I, _____
(User's Printed Name) (User's Social Security Number)

_____
(User's work phone number) (Print User's work street address)

_____
(Print User's employer) (Print User's work email)

acknowledge that I will be assigned a personal User ID and password to gain access to the Texas Workforce Commission (TWC) computer system. Under no circumstances will I allow my User ID or password to be used by any other individual, nor will I use one belonging to anyone else. As an online User with access to confidential TWC data ("TWC Information"), I understand that I will be held personally accountable for my actions and for any activity performed under my User ID. I understand that the use of TWC Information is limited to the following "Limited Purpose(s)" only: _____. I understand that TWC maintains a record of the individuals and employers whose TWC Information I gain access to, and that I am not allowed access to TWC Information about any individual or employer except as necessary for the Limited Purpose(s). I understand that I am not allowed access to TWC Information about myself.

I will not enter any unauthorized data or make any changes to data. I will not disclose any TWC Information orally, electronically, in written or printed form, or in any other manner without prior written authorization from TWC. I will not disclose any TWC Information to other governmental entities, including law enforcement entities.

I understand that under Texas Labor Code §301.085, all TWC Information I obtain under this User Agreement is confidential and that it is a criminal offense to solicit, disclose, receive or use, or to authorize, permit, participate in, or acquiesce in another person's use of TWC Information that reveals: (1) identifying information regarding any individual or past or present employer; or (2) information that foreseeably could be combined with other publicly available information to reveal identifying information regarding any individual or past or present employer. This offense is punishable by as much as a year in jail, a fine up to $4,000, or both.

I understand that under Texas Penal Code §33.02(a), it is a criminal offense to knowingly access a computer, computer network, or computer system without the effective consent of the owner. Depending on the circumstances, the offense is punishable by confinement in jail for up to 180 days or up to 99 years or life in prison, a fine of up to $2,000 or up to $10,000, or both.

I have read and had explained to me the confidentiality and security requirements of 20 C.F.R. § 603.9 and of my employer's contract with TWC. I understand and agree to abide by these requirements. I understand that if I violate any of these requirements or any provision of this User Agreement, I will jeopardize my employer's contract with TWC.

_____
Signature of User Date signed

Supervisor Approval: I have instructed the User listed above about all confidentiality requirements applicable to TWC Information obtained under the contract with TWC, including the requirements of 20 C.F.R. § 603.9 and the sanctions specified in the Contract and in state law for unauthorized disclosure of TWC Information.

_____
Signature of Supervisor Printed Name Date signed

Approval of Contract Signatory or Contact Person named in Contract:

_____
Signature of Contract Signatory or Recipient Contact Person Printed Name Date signed

All fields on this User Agreement are required. Employer must retain signed original and give a copy to User. Employer must send copy of executed User Agreement to TWC EAGLE Administration as specified on the required Cover Sheet, Attachment D to this Contract. An incomplete User Agreement will be rejected.

(Keep only for PENs and PEBs, and NFAs with online access) **Attachment D**

TRANSMITTAL COVER SHEET
FOR NEW USER AGREEMENTS AND TRAINING CERTIFICATES
AND EXISTING USER TRAINING CERTIFICATES

To: **EAGLE Administration**

___ via email to: EAGLEsupport@twc.texas.gov
(Document must be scanned and **encrypted** before sending)

___ via fax to: **512-463-6394**
Number of pages including cover sheet: _____

___ via mail to: **EAGLE Administration**
Texas Workforce Commission
101 East 15th Street, Room 0108
Austin, TX 78778-0001

From: _____ (Recipient Contact Person)

_____ (Recipient Contact Person email)

Re: **User Agreement(s) and Training Certificate(s) attached**

Instructions:

- User Agreement and Training Certificate must be submitted together for each individual.
- Only one cover sheet is required if submitting documents for more than one User at the same time.

For questions regarding the User Agreement, please email EAGLEsupport@twc.texas.gov
Note: An incomplete User Agreement will be rejected

(Keep only for PEFs and PEBs, and NFAs with offline access) **Attachment E**

REQUEST FOR TEXAS WORKFORCE COMMISSION RECORDS

To: External Data Exchange Contracts (EDEC)
Procurement and Contract Services Department
Texas Workforce Commission
1117 Trinity Street, Room 342T
Austin, TX 78701

or via email to: DEContracts@twc.texas.gov

or via fax to: 512-936-0219
Number of pages including cover sheet: _____

From: _____ (printed name of individual submitting request. Note: this person must be Recipient's Contact Person named in Exhibit 1, Request and Safeguard Plan, or a person authorized in writing, on file with TWC, to submit offline requests)

_____ (signature)

_____ (email of point of contact)

_____ (phone)

REQUEST FOR RECORDS

1. Requests must be consistent with the contract **Exhibit 1, Request and Safeguard Plan**, including the description of information requested, safeguards, and method, and frequency of transfer.

2. Describe information requested: E.g., Wage Records

3. Time period of records requested:

(If changes are requested here in this form from the existing Exhibit 1, a new Exhibit 1 will need to be submitted for review and approval and a contract amendment issued.)

For questions regarding this request: DEContracts@twc.texas.gov

Texas Workforce Commission **Attachment F**

Certificate of Destruction for Contractors and Vendors

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The TWC tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization.
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

Contact Name	Title	Company Name and Address	Phone

You may attach an inventory of the media if needed for bulk media disposition or destruction.

Media Type				Media Title / Document Name
	HARD COPY		ELECTRONIC	
Media Description (Paper, Microfilm, Computer Media, Tapes, etc.)				
Dates of Records				

Document / Record Tracking Number	TWC Item Number	Make / Model	Serial Number

Item Sanitization		CLEAR	Who Completed?		Who Verified?	
		PURGE	Phone		Phone	
		DESTROY	DATE Completed			
Sanitization Method and/or Product Used →						
Final Disposition of Media		Reused Internally			Destruction / Disposal	
		Reused Externally			Returned to Manufacturer	
		Other:				

Comments:

If any TWC Data is **retained**, indicate the type of storage media, physical locations(s), and any planned destruction date.

Description of TWC Data Retained and Retention Requirements:

Proposed method of destruction for TWC approval:	
	Type of storage media?
	Physical location?
	Planned destruction date?

Within five (5) days of destruction or purging, provide the TWC with a signed statement containing the date of clearing, purging or destruction, description of TWC data cleared, purged or destroyed and the method(s) used.

Authorized approval has been received for the destruction of media identified above and has met all TWC Records Retention Schedule requirements including state, federal and/or internal audit requirements and is not pending any open records requests.

Records Destroyed by:			Records Destruction Verified by:	
Signature	Date		Signature	Date

Be sure to enter name and contact info for who completed the data destruction and who verified data destruction in the fields above.

Send the signed Certificate of Destruction to:
TWC: Information Security Office, Rm. 0330A, 101 E. 15th Street, Austin, TX 78778-0001

GP Revised: 09-02-15

Texas Workforce Commission **Attachment F**

Certificate of Destruction for Contractors and Vendors

INSTRUCTIONS FOR CERTIFICATE OF DESTRUCTION

Hard copy and electronic media must be sanitized prior to disposal or release for reuse. The TWC tracks, documents, and verifies media sanitization and disposal actions. The media must be protected and controlled by authorized personnel during transport outside of controlled areas. Approved methods for media sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization.
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

IRS Publication 1075 directs us to the FISMA requirements and NIST guidelines for sanitization and disposition of media used for federal tax information **(FTI).** These guidelines are also required for sensitive or confidential information that may include personally identifiable information **(PII)** or protected health information **(PHI).** NIST 800-88, Appendix A contains a matrix of media with minimum recommended sanitization techniques for clearing, purging, or destroying various media types. This appendix is to be used with the decision flow chart provided in NIST 800-88, Section 5.

There are two primary types of media in common use:

- **Hard Copy**. Hard copy media is physical representations of information. Paper printouts, printer and facsimile ribbons, drums, and platens are all examples of hard copy media.
- **Electronic (or soft copy).** Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in NIST SP 800-88, Appendix A.

1. For media being reused within your organization, use the **CLEAR** procedure for the appropriate type of media. Then validate the media is cleared and document the media status and disposition.

2. For media to be reused outside your organization or if leaving your organization for any reason, use the PURGE procedure for the appropriate type of media. Then validate the media is purged and document the media status and disposition. Note that some **PURGE** techniques such as degaussing will typically render the media (such as a hard drive) permanently unusable.

3. For media that will not be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

4. For media that has been damaged (i.e., crashed drive) and cannot be reused, use the **DESTRUCTION** procedure for the appropriate type of media. Then validate the media is destroyed and document the media status and disposition.

5. If immediate purging of all data storage components is not possible, data remaining in any storage component will be protected to prevent unauthorized disclosures. Within twenty (20) business days of contract expiration or termination, provide TWC with a signed statement detailing the nature of TWC data retained type of storage media, physical location, planned destruction date, and the proposed methods of destruction for TWC approval.

6. Send the signed Certificate of Destruction to:

Texas Workforce Commission
Information Security Office
Room 0330A
101 E. 15th Street
Austin, TX 78778-0001

FAX to: 512-463-3062

or send as an email attachment to:

ciso@twc.texas.gov

Final Distribution of Certificate	Original to:	Chief Information Security Officer
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. TWC Contract Manager

GP Revised: 09-02-

Attachment G

QUARTERLY SELF-ASSESSMENT REPORT

Failure to submit this report by due date can result in termination of all access to TWC Information.

The period covered is -Year: _____ Quarter ☐ Q1, ☐ Q2, ☐ Q3, ☐ Q4

The entity receiving TWC Information under TWC Contract ("Recipient") confirms it is in compliance with the requirements of the Contract and the *Safeguards for TWC Information* (Attachment B of the Contract), during the previous period, to include the following:

1. Recipient used the disclosed TWC Information only for purposes authorized by law and consistent with the Limited Purpose set forth in Exhibit 1. Request and Safeguard Plan of the Contract.	Yes: __ No: __
2. Recipient stored the disclosed TWC Information in a place physically secure from access by unauthorized persons. This includes hard copies of the information.	Yes: __ No: __
3. Recipient stored and processed disclosed TWC Information maintained in electronic format outside of the recipient computer systems in such a way that unauthorized persons cannot obtain the TWC Information by any means.	Yes: __ No: __
4. Recipient took precautions to ensure that only authorized personnel were given access to disclosed TWC Information that is stored in recipient's computer systems.	Yes: __ No: __
5. Recipient has instructed all personnel having access to the disclosed TWC Information about confidentiality requirements, the requirements of 20 C.F.R. § 603.9 found in *Safeguards for TWC Information* (Attachment B), and the sanctions specified in State law for unauthorized disclosure. (Each violation is a Class A Misdemeanor, punishable by a fine of $4,000, a year in jail, or both).	Yes: __ No: __
6. Recipient adhered to confidentiality requirements and procedures that are consistent with and meet the requirements of the TWC Contract.	Yes: __ No: __
7. Recipient agreed to report any infraction(s) of these requirements and procedures to TWC fully and promptly.	Yes: __ No: __
8. Recipient disposed of disclosed TWC Information, and any copies thereof made by Recipient, after the purpose for which the TWC Information was disclosed, is served, or as required by court order. (Disposal means return of the TWC Information to TWC or destruction of the TWC Information, as directed by TWC. Disposal includes deletion of personal identifiers in lieu of destruction.)	Yes: __ No: __
9. Recipient ensured that the disclosed TWC Information is not retained with personal identifiers for longer than such period of time as TWC deems appropriate.	Yes: __ No: __
10. Recipient maintained a system sufficient to allow an audit of compliance with the requirements of 20 C.F.R. § 603.9 found in *Safeguards for TWC Information* (Attachment B) and the TWC Contract.	Yes: __ No: __

11. Attached is a description of the system referred to in Item 10. Recipient ensured that any copies of any logs sent to TWC do not contain Sensitive PII. Remember to secure originals containing PII.	Yes: __ No: __
12. Recipient maintained as a minimum, the encryption requirements of FIPS 140-2 and encrypt the data at the minimum of 256-bit AES encryption.	Yes: __ No: __
13. Annual Renewal of Contract User Agreement and training certifications per the Contract terms are on file and copies have been submitted to EAGLEsupport@twc.texas.gov.	Yes: __ No: __
14. All users have completed the training within the previous 12 months.	Yes: __ No: __
15. Is the data received re-disclosed to any other entity? If yes, Receiving Agency ensures that contract personnel are held to the same standard of processing, training, and protecting information as Recipient Agency employees who have a need to use the TWC information for the Limited Purpose. **Express written contract language authorizing data exchange with non-employees is required for redistribution of information accessed**	Yes: __ No: __ Yes: __ No: __

By signature hereon, the Contract signatory or the entity's internal auditor certifies that:

All statements and information submitted in response to this Quarterly Self-Assessment Report are current, accurate, and complete.

_____ _____
Signature Date

_____
Printed Name and Title

Return this Report to:

External Data Sharing Contracts Manager | Procurement and Contract Services Department |
Texas Workforce Commission | 1117 Trinity Street, Room 342T | Austin, Texas 78701

Email: SelfAssessmentReports@twc.texas.gov

Fax: 512-936-021