

**TEXAS WORKFORCE COMMISSION**

**INFORMATION RELEASE CONTRACT AMENDMENT**

INFORMATION RELEASE							
<b>TWC Contract Number</b>	2916PEN010	<b>Amendment Number</b>	2	<b>Effective Date</b>	August 28, 2017		
Recipient Information							
Name	Williamson County Constable Precinct 2						
Mailing Address	350 Discovery Blvd, Ste. 205						
City/State/Zip	Cedar Park, TX 78613						
Telephone Number	(512) 260-4270						
Remarks							
This amendment is contingent on Williamson County Constable Precinct 2's acceptance of and compliance with the terms and conditions of this Information Release Amendment and any referenced attachments.							
Amendment Detail							
Contract Period							
<input checked="" type="checkbox"/> The Contract Period is amended as follows: <div style="display: flex; justify-content: space-around;"> <span>Current End Date: <u>August 31, 2017</u></span> <span>Amended End Date: <b><u>August 31, 2018</u></b></span> </div> <input type="checkbox"/> There are <b>no</b> changes to the Contract Period pursuant to this amendment.							
General Terms and Conditions							
<input checked="" type="checkbox"/> The General Terms and Conditions are amended as follows: <ul style="list-style-type: none"> <li>• Revised Table of Contents. Change is in bold.</li> </ul> <input type="checkbox"/> There are <b>no</b> changes to the General Terms and Conditions pursuant to this amendment.							
Attachment A: Statement of Work - Project Obligations							
<input checked="" type="checkbox"/> Attachment A: Statement of Work - Project Obligations is amended as follows: <ul style="list-style-type: none"> <li>• Revised Sections 1.2, 3.2.1, and 4.1. Changes are in bold.</li> </ul> <input type="checkbox"/> There are <b>no</b> changes to the Statement of Work - Project Obligations pursuant to this amendment.							
Contract Amount							
<input checked="" type="checkbox"/> Contract amount is amended as follows: <ul style="list-style-type: none"> <li>• Increase contract amount by \$1,500.00</li> </ul> <input type="checkbox"/> There are <b>no</b> changes to the contract amount pursuant to this amendment.					<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: center;">Total Amended Contract Amount</th> </tr> <tr> <td style="text-align: center; font-weight: bold;">\$4,500.00</td> </tr> </table>	Total Amended Contract Amount	\$4,500.00
Total Amended Contract Amount							
\$4,500.00							
Changes to Other than the Above Categories							
<input checked="" type="checkbox"/> Other: Attachments B, C, D, G and Attachment H. <ul style="list-style-type: none"> <li>• Revised Attachment B: Sections 2, 7, and 18.</li> <li>• Revised Attachment C: Reworded purpose to match Request and Safeguard Plan (no change in meaning).</li> <li>• Revised Attachment D: Email address is updated,</li> <li>• Revised Attachment G: Formerly <i>Protection of Confidentiality – 20 C.F.R §603.9</i>, now <i>Certificate of Destruction for Contractors and Vendors</i>.</li> <li>• Revised Attachment H: Instructions and Question 5.</li> </ul> <input type="checkbox"/> There are <b>no</b> other changes to the document pursuant to this amendment.							

**Signature Authority**

The person signing this contract amendment on behalf of Williamson County Constable Precinct 2 hereby warrants that he or she has been fully authorized by the organization to:

- Execute this grant award amendment on behalf of the organization, and
- Validly and legally bind the organization to all the terms, performances, and provisions of this contract amendment.

<b>Amendment Approval</b>	<b>Amendment Acceptance</b>
Agency: <b>Texas Workforce Commission</b>  <i>Lisa Richardson</i> _____ Lisa Richardson Date Chief Information Officer	Recipient: <b>Williamson County Constable Precinct 2</b>  _____ Dan Gattis Date County Judge

## TABLE OF CONTENTS

General Terms and Conditions	
Section 1	Purpose and Legal Authority
Section 2	Term, Termination, and Amendment
Section 3	Consideration
Section 4	Protecting the Confidentiality of TWC Information
Section 5	Records and Audit
Section 6	Breach of Agreement, Default, and Remedies
Section 7	Miscellaneous
Attachment A	Statement of Work – Project Obligations
Attachment B	Safeguards for TWC Information
Attachment C	Texas Workforce Commission User Agreement
Attachment D	Cover Sheet for Transmitting User Agreement and Training Certificate
Attachment E, F	<i>“Intentionally omitted”</i>
<b>Attachment G</b>	<b>Certificate of Destruction for Contractors and Vendors</b>
Attachment H	Quarterly Self-Assessment Report

**INFORMATION RELEASE CONTRACT BETWEEN TEXAS WORKFORCE COMMISSION  
AND  
WILLIAMSON COUNTY CONSTABLE PRECINCT 2  
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 solely for the following purpose: **to assist in criminal investigations; to assist in locating defendants, witnesses and fugitives in criminal cases; and to assist in locating persons with outstanding warrants** (the “Limited Purpose”). 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 Online Access.
- 2.1.1 Description. Agency agrees to provide online "read-only" access to the following Agency mainframe computer screens:
- BN75: wage records file;
  - CMES, CTCS, and BPCS: unemployment compensation claim benefit data
- 2.1.2 Number of Users. Subject to Section 3.1, Agency will grant access to the screens listed in Section 2.1.1 to a maximum of ten (10) “Users,” all of whom must be direct Recipient employees.
- 2.1.3 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.

### SECTION 3 – Obligations of Recipient

#### 3.1 Online Access.

- 3.1.1 Annual Fee and Payment. Recipient shall pay Agency a one thousand five hundred dollars (\$1,500.00) annual subscription fee for the online access described in Section 2.1. 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) 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. Recipient shall pay agency the annual subscription fee for each subsequent contract year within thirty (30) days of the beginning of each contract year. Recipient shall send payment to Texas Workforce Commission, Revenue and Trust Management, P.O. Box 322, Austin, TX 78767-0322.
- 3.1.2 User Documents. All prospective online Users must execute a *Texas Workforce Commission User Agreement* ("User Agreement"), Attachment C, and complete online TWC Information Technology Security Awareness Training ("Security Training").
- 3.1.3 User Document Submission and Maintenance. Before Agency RACF Administration will issue a User ID and password to a prospective User, Agency RACF Administration must receive from Recipient Contact Person (designated in Section 4.1) copies of a completed User Agreement and certificate of completion of Security Training ("Training Certificate"), with a completed *Cover Sheet for Transmitting User Agreement and Training Certificate* ("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.
- 3.1.4 Annual User Renewal. Each year, on the first day of the month following the anniversary of the Begin Date, the online access of each User will be terminated unless Agency RACF Administration has received for the User, 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.
- 3.1.5 Notice of User Employment Change. Recipient shall notify Agency 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.
- 3.1.6 User Document Renewal. On October 1, 2015 the online access of each User established under a prior contract will be terminated unless Agency RACF Administration has received for the User, 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.
- 3.1.7 Changes 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.

3.1.8 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 Additional Requirements.

3.2.1 **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.

3.2.2 Suspension. Agency may suspend all services without notice if Agency suspects a violation of the security 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 Self-Assessment Report. Recipient shall submit to Agency a fully-executed *Quarterly Self-Assessment Report*, Attachment H, 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 1, April 1, July 1, and October 1. Each report must have been signed within thirty (30) days preceding submission.

3.2.7 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.

3.2.8 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.

- 3.2.9 Computer Resources. Recipient shall provide and maintain its own computer hardware and software to accomplish the necessary computer communications linkages with Agency.
- 3.2.10 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 following primary liaisons for implementation of this Contract:

##### Agency Contact Person

M. Sonja Elizondo  
External Data Exchange Contracts (EDEC)  
Procurement and Contract Services Department  
Texas Workforce Commission  
1117 Trinity Street, Room 304T  
Austin, TX 78701

Phone: (512) 463-0291  
Fax: (512) 936-0219  
Email: [Sonja.Elizondo@twc.state.tx.us](mailto:Sonja.Elizondo@twc.state.tx.us)

##### Recipient Contact Person

**William H. Beechinor**  
Chief Deputy  
Williamson County Constable Precinct 2  
350 Discovery Blvd., Suite 205  
Cedar Park, TX 78613

Phone: (512) 260-4270

Email: [wbeechinor@wilco.org](mailto:wbeechinor@wilco.org)

Send invoices to:

Same as above

- 4.2 Notice. Any notice required under this Contract must be given to the other Party's Contact Person.
- 4.3 Notice to Alternate. If Recipient designates an alternate Contact Person, 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 – Effect on Other Contracts**

The Parties agree that this Contract supersedes and replaces all other contracts between them for information release or data sharing, including 2913PEN069.

Remainder of Page Intentionally Left Blank



## 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”: **to assist in criminal investigations; to assist in locating defendants, witnesses and fugitives in criminal cases; and to assist in locating persons with outstanding warrants**. 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 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 G, 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; 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.
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* (Attachment B of this Contract) relating to safeguarding TWC Information and insuring 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 encryption.
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.

**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 only: **to assist in criminal investigations, to assist in locating defendants, witnesses and fugitives in criminal cases, and to assist in locating persons with outstanding warrants.** 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. 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 knowingly to access a computer, computer network, or computer system without the effective consent of the owner. Depending on the circumstances, the offense is punishable by 180 days in jail up to 99 years or life in prison, a fine of \$2,000-\$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 agreement are required. Employer must retain signed original and give a copy to User. Employer must send copy of User Agreement to TWC RACF Administration as specified on the required Cover Sheet, Attachment D to this Contract.

**COVER SHEET FOR TRANSMITTING USER AGREEMENT AND TRAINING CERTIFICATE**

To: **RACF Administration**

\_\_\_ via email to: [racfadm@twc.state.tx.us](mailto:racfadm@twc.state.tx.us)  
(Document must be scanned and **encrypted** before sending)

\_\_\_ via fax to: **512-463-6394**  
Number of pages including cover sheet: \_\_\_\_\_

\_\_\_ via mail to: **RACF Administration**  
Texas Workforce Commission  
101 East 15<sup>th</sup> Street, Room 0330  
Austin, TX 78778-0001

From: **Williamson County Constable Precinct 2** (Recipient)

\_\_\_\_\_ (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.
- An incomplete User Agreement will be rejected.
- **For questions regarding the User Agreement, please email [racfadm@twc.state.tx.us](mailto:racfadm@twc.state.tx.us)**

Texas Workforce Commission  
**Certificate of Destruction for Contractors and Vendors**

Revised Attachment G

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. <a href="http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf">http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf</a>				
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		
<input type="checkbox"/> HARD COPY	<input type="checkbox"/> 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	<input type="checkbox"/> CLEAR	Who Completed?		Who Verified?
	<input type="checkbox"/> PURGE	Phone		Phone
	<input type="checkbox"/> DESTROY	DATE Completed		
Sanitization Method and/or Product Used →				
Final Disposition of Media	<input type="checkbox"/>	Reused Internally	<input type="checkbox"/>	Destruction / Disposal
	<input type="checkbox"/>	Reused Externally	<input type="checkbox"/>	Returned to Manufacturer
	<input type="checkbox"/>	Other:		
<b>Comments:</b>				
If any TWC Data is <b>retained</b> , indicate the type of storage media, physical locations(s), and any planned destruction date.				
<b>Description of TWC Data Retained and Retention Requirements:</b>				
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	
<b>Be sure to enter name and contact info for who completed the data destruction and who verified data destruction in the fields above.</b>				
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  
**Certificate of Destruction for Contractors and Vendors**

Revised Attachment G

**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](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 platen 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. 15<sup>th</sup> Street  
 Austin, TX 78778-0001

FAX to: 512-463-3062

or send as an email attachment to:

[willie.harvey@twc.state.tx.us](mailto:willie.harvey@twc.state.tx.us)

Final Distribution of Certificate	Original to:	Willie Harvey, Chief Information Security Officer 512-463-8372
	Copy to:	1. Your Company Records Management Liaison - or - Information Security Officer 2. TWC Contract Manager

GP Revised: 09-02-15

**QUARTERLY SELF-ASSESSMENT REPORT**

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

**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 Section 1.2 of Attachment A 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: __
<b>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 <i>Safeguards for TWC Information</i> (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).</b>	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 (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 <a href="mailto:RACFAdmn@twc.state.tx.us">RACFAdmn@twc.state.tx.us</a> .	Yes: __ No: __
14. All users have completed the training within the previous 12 months.	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

**Williamson County Constable Precinct 2  
2916PEN010-2**

**Return this Report to:**

External Data Sharing Contracts Manager | Procurement and Contract Services Department |  
Texas Workforce Commission | 1117 Trinity Street, Room 304T | Austin, Texas 78701

Email: [SelfAssessmentReports@twc.state.tx.us](mailto:SelfAssessmentReports@twc.state.tx.us)

Fax: 512-936-0219