**TEXAS WORKFORCE**

**COMMISSION**

**External Data Exchange**

**Data Customer**

**User Guide**

**Version 1.0**

**Revised September 2025**



 Table of Contents

[Section I Introduction 2](#_Toc208227158)

[1.1 Overview 2](#_Toc208227159)

[1.2 What can a DC use the UI data for? 3](#_Toc208227160)

[1.3 How to Use this User Guide 4](#_Toc208227161)

[1.4 Version Control 4](#_Toc208227162)

[1.5 Principles and Outcomes 4](#_Toc208227163)

[Section II Overview 5](#_Toc208227164)

[2.1 EDE Data Types 5](#_Toc208227165)

[2.2 Methods of Disclosure 6](#_Toc208227166)

[2.3 Laws Relating to Disclosure of Records 10](#_Toc208227167)

[Section III Application Process 10](#_Toc208227168)

[3.1 Process Map 10](#_Toc208227169)

[3.2 Definitions 12](#_Toc208227170)

[3.3 Exhibit 1, TWC Data Exchange RSP 13](#_Toc208227171)

[Instructions 13](#_Toc208227172)

[3.3.1 General Overview for Offline and Online Requests 13](#_Toc208227173)

[3.3.2 Offline RSP Instructions 14](#_Toc208227174)

[3.3.3 Online RSP Instructions 27](#_Toc208227175)

[Section IV QSAR 41](#_Toc208227176)

[4.1 Online QSAR Instructions 41](#_Toc208227177)

[4.2 Offline QSAR Instructions 45](#_Toc208227178)

[Section V Data Disposal 48](#_Toc208227179)

[5.1 Data Destruction and De-Identification Requirements 48](#_Toc208227180)

[5.2 Compliance with Standards 49](#_Toc208227181)

# Section I Introduction

## 1.1 Overview

The Texas Workforce Commission (TWC) holds confidential data to which external parties are granted access to meet the entities mission. When TWC agrees to provide confidential data to a Data Customer (DC), it is through an External Data Exchange (EDE) agreement. Inside TWC, staff and procedures handle all aspects of sharing data, through the EDE system.

Most DCs are seeking data from the Unemployment Insurance (UI) program. UI data includes the Wage and Tax Statement (Form W2) information as well as benefits paid to UI claimants. UI data is always confidential. To access UI data, a DC must apply, show they qualify under the law, obtain TWC’s agreement that they are eligible, sign an EDE contract, and comply with the conditions and restrictions.

The Code of Federal Regulations, 20 CFR § 603.9, states only a handful of vetted and qualified DCs will be allowed to access UI data. Federal law requires TWC to recover costs associated with granting access and maintaining the EDE system. The charge in the EDE contract is the amount necessary for TWC to recover the cost of providing the data. Compared to the high value of the UI data, the charge is nominal and does not include any profit to TWC. TWC does not sell data or subscriptions.

## 1.2 What can a DC use the UI data for?

This section addresses a critical distinction in how UI data must be handled under federal law. Unlike most public information obtained from state government, UI data is subject to strict confidentiality requirements and cannot be used at will, retained, or shared freely.

When requesting access to UI data, TWC is legally required to ask the purpose of the request. The potential DC must provide a written description of the intended use. If a data sharing agreement is approved, the DC is strictly limited to using the UI data only for the purpose stated in writing and authorized by TWC.

UI data may not be repurposed or shared with other parties unless such activity is explicitly documented in the application and approved in advance. Once the approved use has concluded, the DC must dispose of the UI data in a manner that complies with TWC’s standards. This includes documenting the disposal process and submitting that documentation to TWC for verification.

## These requirements are not optional and are enforceable under federal law. DCs must ensure full compliance throughout the duration of the agreement and beyond.

## 1.3 How to Use this User Guide

This User Guide provides a general overview of EDE contracts and relevant TWC procedures. While it offers instructions on the contract application process, completing the Exhibit 1, the TWC Data Exchange Request and Safeguard Plan (RSP), and accessing post-contract forms, it is not an exhaustive resource for all possible transaction-specific scenarios.

## 1.4 Version Control

This User Guide was first published in 2025. When modifications are made, the version number on the cover page of the User Guide will be updated and the version history will be revised to include a summary of the revisions.

## 1.5 Principles and Outcomes

TWC is committed to safeguarding its electronic data, particularly UI data, through a combination of legal compliance, operational discipline, and technical standards. This commitment includes adherence to federal confidentiality regulations, such as 20 C.F.R. Part 603, and alignment with recognized frameworks like those issued by the National Institute of Standards and Technology (NIST). UI data is considered confidential at all times, including within TWC, and is not shared or repurposed outside the UI system unless a specific exception is granted. These exceptions are rare and must be justified, documented, and approved through a formal process. TWC applies a default presumption of denial to all external requests for UI data. To be considered for access, a DC must submit a formal application that establishes legal eligibility, demonstrates a clear commitment to comply with all applicable restrictions and safeguards, and includes written authorization from TWC’s Executive Director or their designee.

TWC conducts a thorough review of each application and excludes any applicant who does not meet the required criteria. While TWC recognizes its data is uniquely valuable and often sought for purposes that cannot be fulfilled through other sources, these factors alone do not justify access. Applicants are encouraged to present a complete and well-supported case. If an application appears incomplete or inaccurate, TWC will notify the applicant and provide an opportunity to clarify or submit additional documentation. If the applicant is unable or unwilling to meet the necessary standards, the application will be denied. This process ensures that TWC’s data remains protected while allowing qualified applicants to pursue access through a structured, transparent, and legally compliant framework.

# Section II Overview

## EDE Data Types

TWC allows federal, state, and local governments and agencies and their delegated proxies/agents to contract with TWC through an EDE contract for access to TWC’s automated systems to gather data to meet their requirements. The system(s) covered by EDE contracts contain sensitive and/or confidential data and include:

1. Tax - quarterly wage amounts earned by individuals as well as the name and address of each employer. Employer information can include a list of people who work at a specific company and individual information of key employees. Benefits - unemployment benefits paid to individuals (i.e., claimants). Benefits-related information also includes each claimant’s address, birth date, and other personal information.
2. Work in Texas (WIT) - job matching information including job postings and job applicant information.
3. The Workforce Information System of Texas (TWIST) - participant information in workforce services including the Workforce Innovation and Opportunity Act (WIOA), the Child Care & Early Learning Program, the Choices Program, and the Supplemental Nutrition Assistance Program Employment and Training Program (SNAP E&T).

## 2.2 Methods of Disclosure

Through an EDE contract, TWC may provide access to information via online or offline request.

1. Online access – Remote external access through the External Agency and Law Enforcement (EAGLE) portal to those who wish to access data directly from TWC’s system.
2. Offline access – Customized reports (ad hoc) can be obtained via scheduled data transfers using secure file transfer protocols.

## 2.3 Access to Information Contained in Unemployment Insurance Records

The information maintained by TWC, as administrator of the unemployment insurance program, is confidential and not subject to public disclosure. There is an exception to this confidentiality requirement for public officials who need the information for the administration or enforcement of a law. The public official must agree to maintain the confidentiality of the information obtained from TWC.

The request from the public official must be made in writing on official letterhead. The request must identify the requester as a public official, must include a statement that the information requested is necessary for the administration or enforcement of a law, must list the specific purpose for which the information will be used, and must be signed. The requester must also sign a TWC confidentiality agreement.

**Data Sharing Agreements**

If the public official anticipates an ongoing need for access to TWC records, TWC will prepare a contract to facilitate access. The contract can be for online access, off-line access, or both.

**Costs**

There is a charge for providing information maintained as part of the Unemployment Insurance program. TWC can recover the cost of providing this information to authorized agencies. The costs depend on the method provided and the amount and frequency of data provided.

**Method of Receiving Data**

**1) Online Access**

The charge for online access to TWC unemployment compensation information (including wage records, unemployment compensation benefits information, and employer tax information) will be based on a yearly subscription fee. The yearly subscription fee will be determined by the number of users authorized in the contract to access information online. Payment of the yearly fee must be received by TWC by the due date listed in the contract. The yearly fee will cover basic online access charges for a twelve-calendar month period starting on the begin date listed in the contract.

Rate Schedule for online access:

|  |  |
| --- | --- |
| **Number of Authorized Users** | **Annual Subscription Rate** |
| 1-10 | $3,750 |
| 11-25 | $5,000 |
| 26-50\* | $8,750 |
| 51-100\* | $15,000 |
| 100-500\* | $62,500 |
| 501-1,000\* | $125,000 |
| 1,001-2,000\* | $250,000 |
| 2,001-3,000\* | $375,000 |
| Over 3,000\* | $500,000 |

\*If a contractor wants more than 25 users a year, it must submit a written justification explaining why more than 25 users is needed and must obtain written approval of the number by TWC.

**2) Offline Access**

Rate Schedule for SSNs provided by requester to match against TWC wage records:

|  |  |
| --- | --- |
| Processing Fee | Fee Per Job |
| 1-999 | $625 |
| 1,000 – 14,999 | $750 |
| 15,000 – 19,999 | $935 |
| 20,000 – 24,999 | $1,250 |
| 25,000 and above | $2,500 |

Programming Fee

In addition to the rate schedule above, an hourly rate is charged for time utilized by programmers and system analysts in the Information Technology department. The below rate will be multiplied by the total hours spent on creating new requests/jobs or modifying existing requests/jobs that were previously created.

|  |  |
| --- | --- |
| Costs for New or Modification of Existing Jobs | Fee Per Job |
| Programming Services | $93.51 |

Offline Request Specifications

Data available to match include Social Security number, Texas Employer ID, Federal Employer Identification number. This will be provided to TWC via a seed file. Requesting different data elements must be discussed with the contract manager to determine if data is available to share.

**3) Access to both – Online and Offline**

You may choose to have access to both methods. The cost is a combination of both.

**Request a Contract**

The contracting process begins with the submission of the Request and Safeguard Plan (RSP) form. A copy of this form is attached to the email on which this document was sent.

If you have further questions, please contact External Data Exchange at: DEContracts@twc.texas.gov.

## 2.4 Laws Relating to Disclosure of Records

Unemployment compensation information including wage records, employer tax records, and unemployment insurance benefits claims may be confidential and have limited disclosure under the following:

1. Regulations at 20 Code of Federal Regulations (CFR) Part 603;
2. Texas Labor Code §§ 301.081 – 301.085; 40 Texas Administrative Code §§ 815.161 – 815.168; and
3. Guidance from the NIST’s Special Publication NIST SP 800-188 for de-identifying government datasets.

# Section III Application Process

## 3.1 Process Map

The following process map provides a detailed breakdown of the TWC EDE application process. Please review this map carefully to understand the steps involved.

## Definitions

1. “CII” means Confidential Identifiable Information. Per federal law, CII is any data “which reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with any other publicly available information to reveal any such particulars.” 20 CFR 603.4(b).
2. “Data Customer (DC)” and “Recipient” both mean the legal entity identified as a party to the External Data Exchange Contract.
3. “EAGLE” refers to TWC’s web-based platform for DCs to have online access to TWC Data, called the External Agency and Law Enforcement (EAGLE).
4. “EDE” refers to External Data Exchange, a structured system and set of agreements for the secure and compliant electronic transmission of sensitive information between organizations, often involving government agencies and external partners. This system typically encompasses standardized data formats, security protocols, and contractual obligations to ensure data integrity and confidentiality.
5. “EDE Contract” or “Contract” refers to the specific signed agreement authorizing the Data Customer to receive data from TWC. It can be either an Online Information Release Contract or an Offline Information Release Contract.
6. “Limited Purpose” is defined by Recipient’s responses to Limited Purpose section in the RSP.
7. “Online Access” and “Offline Access” refer to methods for TWC to provide TWC Data to Recipient.
8. “Original TWC Data” means the data set(s) Recipient obtain(s) from TWC. It is data in the form and format prepared by TWC to transmit the data to Recipient. It includes any duplicates or copies of the file(s) received from TWC, as well as all data captured or downloaded from the EAGLE system.
9. “Re-Disclosure” means a Recipient providing access to or copies of any TWC Data to any person who is not an employee of the Recipient or to any entity other than the exact legal entity identified as a Recipient.
10. “RSP” refers to the document attached to the EDE Contract as ***Exhibit 1, TWC Data Exchange Request and Safeguard Plan***. The RSP is TWC’s standard application form to obtain a contract accessing TWC Data. Recipient completes and signs the RSP, and it is attached to this agreement and is incorporated herein.

## 3.3 Exhibit 1, TWC Data Exchange RSP

## Instructions

### **3.3.1 General Overview for Offline and Online Requests**

DCs seeking access to TWC Data must submit a completed RSP to DEContracts@twc.texas.gov. If an RSP application is approved, and leads to a data sharing contract, it will be included in the EDE contract as Exhibit 1.

How an applicant fills out the RSP has legal consequences. Answers will be the basis for eligibility for an EDE contract. When an applicant’s RSP answers become part of a contract, the answers become legally enforceable.

Use the RSP and the following instructions to provide the best answer to each item. Some DC will need to attach supplemental pages. If needed, attach a best draft of each supplemental page.

**Important:** The RSP must be signed by a representative authorized to bind the applicant’s organization to a contract. Consider waiting until the assigned Contract Manager (CM) confirms the accuracy and acceptability of an applicant’s draft answers before obtaining the signature. Changes are not permitted after signing, and a new signature will be required for any revisions requested by the CM.

To complete the RSP, the applicant may need to consult with other people in the organization. Some items ask about Information Technology (IT), Human Resources (HR), legal issues, or other internal process issues. Also, if the Compliance Liaison (CL) is not the person completing the RSP, then they will have to carefully review and approve it. When an item asks the applicant to “specify,” type in the details on the RSP form. If the applicant has more than one or two sentences, consider adding supplemental pages (and note the addition on the RSP).

### **3.3.2** **Offline RSP Instructions**

1. **Exact Legal Name (Item 1)**
	1. The EDE contract will be between TWC and one other legal entity. Provide the name of the other legal entity who will sign the contract. This must be the same entity as the employer of the people who will access and use the TWC Data. This is critically important. If the applicant names an entity other than the employer, the application will be denied. By law, only employees of the entity in Item 1 can access and use the TWC Data.
2. **Tax ID (Item 2)**
	1. TWC is not able to issue a contract without a Tax ID number. It is a required field, as are all items in the application. Applicants may need to contact applicant’s finance or legal department to get the Tax ID number.
3. **DC’s Address (Items 3-5)**
	1. Provide the physical address of the DC.
4. **Seeking Offline Access (Item 6)**
	1. It is the data customer’s responsibility to select the correct RSP for the type of data access it is requesting access for. Refer to Section 2.2 above to differentiate between Offline and Online access. It is the DC’s responsibility to select the correct RSP for the type of data access it is requesting access for. Refer to Section 2.2 above to differentiate between Offline and Online access.
5. **List of Contracts with TWC (Items 7-8)**
	1. Items 7 and 8 request information regarding any existing legal agreements the applicant has with TWC. It is essential to provide accurate TWC assigned contract numbers, as these are unique identifiers used for all TWC contract-related communications. Please list all EDE contract numbers in Item 7 and any other relevant TWC contract numbers in Item 8. Providing this information is crucial for TWC to determine the most appropriate and secure approach for documenting data sharing arrangements with the applicant.
6. **Contract’s Initial Term (Item 9)**
	1. TWC generally prefers contracts with a five (5)-year term, aligning with the maximum duration permitted by the state. However, we recognize that not all agencies have the budgetary capacity to commit to a five (5)-year agreement. Please indicate the desired contract duration in the designated section of the application.
7. **Start Date (Item 10)**
	1. When selecting the checkboxes, please specify if the EDE contract should align with the federal fiscal year or another annual cycle relevant to the applicant. Furthermore, if applying for the contract during the middle of the preferred cycle, please detail the preferred method for aligning future contract years. For example, indicate if the initial contract year is to be less than twelve (12) months to facilitate alignment with the desired annual cycle in subsequent years.
8. **Type of Entity (Item 11)**
	1. Please select only one organizational type. While any organization is eligible to apply for an EDE contract, please be aware that TWC rarely approves RSPs submitted by for-profit or non-profit entities. Most EDE contracts are awarded to governmental entities. Therefore, carefully consider this information when selecting the appropriate option in Item 11.
9. **Contract Authority and Mission of Recipient (Items 12-13)**
	1. Provide a statutory citation demonstrating the applicant’s legal authority to enter into contractual agreements. Some legal entities possess limited or no authority to execute contracts, and all entities operate under a statute that defines their contractual powers, if any. An applicant may need to consult with the legal department to obtain the appropriate legal citation to fulfill this requirement.
	2. For Item 13, select only one (1).
10. **Limited Purpose (Item 14)**
	1. 20 CFR 603 mandates that any use of TWC data requires prior approval. Securing an EDE contract grants the applicant authorization to utilize TWC data solely for the specific purposes and tasks documented and approved within the applicant’s RSPRSP.
	2. Approval for specific data uses is not guaranteed for all DCs. The only way to determine if a particular intended use will be approved in the requested circumstances is to explicitly request it in response to Item 14, enabling TWC to thoroughly evaluate the request. To determine the precise purposes and uses of TWC data within the applicant’s organization, the applicant may need to consult with the individuals who manage or lead the employees utilizing this data.
	3. A critical aspect of TWC's ongoing monitoring is ensuring that TWC data is not used for any purpose that was not disclosed and explicitly approved. Improper or unauthorized data use will trigger TWC's right to legal remedies, including potential termination of the data sharing contract.
11. **Withdrawn Uses (Item 15)**
	1. If this is the initial draft of the RSP, select the "no" box in Item 15. Should the assigned CM subsequently inform the DC that one or more of the uses outlined in the response to Item 14 are not approved, take the following actions in your next draft submission: 1) deselect the disallowed purpose in Item 14, 2) select the "yes" box in Item 15, and 3) provide a comprehensive list of all purposes that were requested but not approved by the CM.
12. **Required Task (Item 16)**
	1. If the applicant is legally obligated through a state or federal statute or other regulatory authority to perform a task that necessitates access to TWC's data, provide a specific citation to the relevant statute, regulation, or authority. Additionally, provide a detailed description of the task the applicant is mandated to complete. Providing this information is crucial for demonstrating the legal basis for the data request.
13. **Charging a Fee to Third Parties (Item 17)**
	1. Regarding the use of TWC Data for determining eligibility for public assistance or public services, please carefully consider the following:
		1. If the applicant will not be utilizing TWC Data in the process of determining eligibility for public assistance or public services, select the first "no" box and proceed to the next section.
		2. If the applicant is a public hospital, public health facility, or determines eligibility for any program or benefit other than public health, and bills patients or beneficiaries for any services or benefits, even in specific situations, the applicant must select "yes" and attach the required supplemental pages. This encompasses any billing or charging to the individual receiving benefits or participating in the program, financial guarantors, family members, or residents in the individual's household. If uncertain about whether or how often individuals are charged in connection with eligibility determinations, select "yes" and attach the supplemental pages.
		3. If the applicant selects "yes," please copy and paste the following statement (including the italics and underlining) at the end of your supplemental pages: “*Accessing, viewing, or using TWC data must be for the sole purpose of making an eligibility determination as described above. No one will use TWC data for any other purpose, task, or program. In particular, TWC’s data must never be used for collections, credit, credit worthiness or accounts payable functions.”*
		4. To ascertain whether the applicant engages in any billing or charging practices, it may be necessary to consult with the applicant’s finance department or the individuals who manage employees who utilize TWC Data.
14. **Information Requested (Item 18)**
	1. Please indicate the type of data report the applicant would prefer to receive. Upon execution of an EDE contract, TWC will provide the applicant with instructions on establishing a Go Anywhere account. The DC will be required to upload a "seed file" containing the Social Security Numbers (SSNs) of the individuals for whom the DC is requesting data, along with unique identifiers for each record. TWC will then return the file, using the unique identifiers you provided, but will omit the SSNs.
15. **Data Transfer and Frequency (Item 19)**
	1. Select the frequency of data requests
16. **Data Request Amount/Size (Item 20)**
	1. Specify the volume or quantity of records the applicant anticipates requesting per submission. It is important to note that TWC will not accept Purchase Orders (POs) from the applicant under this EDE contract. TWC is not selling data or subscriptions, and the applicant is not procuring goods or services from TWC. If a PO is submitted, the applicant will be required to retract it. As required by law, TWC is recovering the cost associated with establishing the EDE contract.
17. **Part A and Part B of Redisclosure (Item 21)**
	1. This section pertains to documenting various aspects of how the applicant manages and handles TWC data within the applicant’s organization. Part A inquires whether individuals other than direct, permanent employees will be *using* the data. Part B asks whether individuals other than direct, permanent employees will have *access* to the data.
	2. If either of these processes involves non-employees, the applicant is required to provide a detailed description by selecting the appropriate checkboxes and providing additional information. TWC approval is mandatory for any such arrangement. If approved, the applicant must acknowledge the acknowledgement box on the RSP and fulfill the associated obligations. The applicant may need to consult with the HR department, IT department, or the individuals who manage employees who use TWC's data to accurately complete this section.
18. **Background Checks (Item 22)**
	1. This section requests information regarding the applicant’s use of background checks to safeguard TWC data. Please describe the current background check practices and how they contribute to protecting the confidentiality and integrity of the data. To provide a complete and accurate response, the applicant may need to consult with the HR department or the individuals who manage employees who use TWC's data.
19. **Outsourcing IT Tasks (Item 23)**
	1. This section addresses the use of outsourcing in the applicant’s IT infrastructure. For the purpose of this document, "outsourcing" refers to situations where individuals performing IT work for the applicant are not employees of the entity named in Item 1. "IT" encompasses all aspects of Information Technology, including the installation, security, and maintenance of the applicant’s hardware and software.
	2. If the applicant exclusively utilizes employees for all IT-related tasks, select the "no" box. However, if any part of the IT system is managed by non-employees, select "yes" and provide comprehensive details, attaching supplemental pages as needed to fully explain the arrangement. The applicant may need to consult with the IT department, Chief Information Security Officer, HR department, or legal department to accurately complete this section.
20. **Data Security Protocols (Item 24)**
	1. Security protocols outline the specifications and detailed guidelines for safeguarding all aspects of the IT system. These protocols establish standards for areas such as firewalls, password management, physical access control, electronic access control, and procedures for handling security breaches.
	2. Item 24 assesses the current state of the applicant’s IT system protection. For Item 24A, indicate whether the applicant has formally committed to a recognized set of security protocols. If so, specify which protocol set has been adopted.
	3. For Item 24B, if applicant has formally adopted a set of security protocols but has not yet fully implemented and achieved compliance, attach supplemental pages describing the specific steps the applicant will take and the timeline for achieving full implementation and compliance.
	4. If, in Item 24A, applicant indicated the applicant has not adopted any recognized set of security protocols, then in Item 24B, select the "no" box and attach supplemental pages detailing the improvements or upgrades the applicant plans to implement within the next six (6) to twelve (12) months.
	5. applicant may need to consult with the auditor, risk manager, Chief Information Security Officer, IT department, or legal department to accurately complete this section.
21. **Assessing Security (Item 25)**
	1. Item 25 requests fundamental information regarding the frequency and methodology employed to assess and confirm that the applicant adheres to the security protocols it has adopted.
	2. Please note that an "attestation" is a distinct document, typically a concise, self-contained record (often one page or less) confirming that a security assessment has been conducted. An attestation is *not* a copy of the assessment results themselves. **Do not submit copies of the applicant’s assessment results to TWC.**
	3. You may need to consult with applicant’s auditor, risk manager, Chief Information Security Officer, IT department, or legal department to accurately complete this section.
22. **Exception to Standard Form (Item 26)**

a. The Quarterly Self-Assessment Report (QSAR) is a comprehensive document that must be submitted to TWC every ninety (90) days, detailing the proactive measures the applicant takes to ensure the proper handling of TWC data. The QSAR requires the submission of specific forms, including a usage log, which applicants are required to maintain using the TWC-provided template. Use of the TWC-provided log form is mandatory.

b. If you utilize case management software or another integrated system to track each instance of accessing the TWC web portal and wish to submit reports generated from that software in lieu of the mandatory log form, indicate the preference in Item 26 and attach supplemental pages showcasing the format and content of the proposed alternative report.

c. Ensure applicant reports do not contain any Personally Identifiable Information (PII) and do not include any data that could enable a third party to ascertain the identity of any search subject (individual or employer). Applicant reports must contain sufficient information to allow to 1) readily retrieve the case file containing the TWC Data accessed during that search if requested by TWC, and 2) enable TWC to identify the date and time of the search for cross-referencing with our internal records.

1. **Disposing of Data (Item 27)**
	1. Federal law (Rule 603) mandates the proper and secure disposal of all TWC data. The Certificate of Destruction for Contractors and Vendors, which outlines the requirements for data disposal, can be found within the EDE User Guide available on the TWC website at <https://www.twc.texas.gov/agency/contract-opportunities>. Please consult [Section 5](#_Section_V_Data) of this document for detailed instructions on compliant data disposal procedures.
2. **Data Encryption (Item 28)**
	1. Select type of data encryption applicant uses to protect TWC data at rest.
	2. Applicant may need to contact the IT department for this information.
3. **Compliance Liaison (Items 29-31)**
	1. TWC approval is required for the designated CL. The CL must be an executive or senior manager within the applicant’s organization identified in Item 1, possessing the authority to address and rectify issues raised by TWC. While the CL can delegate specific tasks, they must serve as the primary point of communication with TWC when requested.
	2. It is important to distinguish between the CL and the Point of Contact (POC). The POC, often an administrative or clerical staff member designated in Item 35, typically manages the day-to-day paperwork and contract administration for the applicant. While most TWC communications will be directed to the POC, the CL will also be copied on certain messages, including formal legal notices.
	3. The CL will be contacted and expected to address situations of a more serious nature, requiring the attention of a higher authority capable of making policy-level decisions to ensure ongoing or restored compliance with the conditions and restrictions outlined in the EDE contract, as well as adhering to federal law.
	4. When selecting the CL nominee, carefully consider the following questions:
		1. Is the individual an executive or upper-level manager within the applicant’s organization?
		2. Does the individual possess the authority to assign tasks to staff and require operational changes within the applicant’s organization?
		3. Do the individual's role and title align with these responsibilities?
		4. Are there other factors demonstrating the individual's suitability for the CL role to TWC's satisfaction?
		5. In the event of a violation of 20 CFR 603, can the individual immediately implement corrective action?
		6. If TWC were to conduct an on-site review of applicant’s performance under the EDE contract, would the individual be able to require staff within the applicant’s organization to provide TWC with all necessary access and information?
		7. If the applicant were at risk of losing its EDE contract due to a breach of contract conditions or restrictions, would this individual have the authority to implement preventative measures to avoid termination?
		8. As a critical example, termination will occur if the POC fails to submit the QSAR on time or fails to complete it correctly.
4. **Contact Information (Items 32-56)**
	1. Provide the required information for the CL, POC, Alternate POC, Signatory (authorized representative signing on behalf of the entity named in Item 1), Data Technology contact, and the designated point of contact for TWC invoices.
	2. As a reminder, the RSP states: "If the application leads to a contract, applicant agrees to provide written notice to TWC of any changes to the responses contained in this RSP immediately but no later than three (3) calendar days from the date of change. Email changes to DEContracts@twc.texas.gov." It is crucial to maintain accurate and up-to-date contact information with TWC throughout the duration of the contract.
5. **Invoices (Item 52)**
	1. Provide the contact information for the individual responsible for receiving invoices from TWC. TWC will send invoices directly to this contact. It is imperative to understand that the applicant should not send a PO for this transaction. This is not a procurement, and TWC is not acting as a vendor selling data, subscriptions, or any other goods or services. An EDE contract constitutes a cooperation agreement, and TWC is obligated under federal law (Rule 603) to recover costs associated with sharing TWC Data.
6. **Signature**
	1. The "attestation" section is located directly above the signature line. By signing the RSP, the applicant is agreeing to and attesting to the accuracy of all responses provided within the document, as well as specifically acknowledging the points outlined in the attestation itself.
	2. Given that responses in the RSP will be legally binding upon the entity named in Item 1, the applicant may wish to have legal counsel review the draft RSP responses before submitting them to TWC.
	3. For many DCs, particularly first-time applicants, it may be prudent to defer signing the draft RSP. While it is not incorrect to sign the draft, please be aware that it is likely a new signature may be required on a revised version following feedback from TWC.

**Important:** The name and title provided in the signature block (and the signed name itself) must precisely match the information provided in Items 44 and 45.

1. **Steps to Complete your RSP**
	1. To complete the application process, fill out the RSP form using only the form itself and these instructions. Provide best possible response for each and every item, ensuring that no items are left blank.
	2. Confirm that the designated CL has reviewed and approved all draft answers, as indicated in Item 30.
	3. Ensure all necessary supplemental pages are attached. Depending on the applicant's specific circumstances, applicant may have no supplemental pages, or may require them for one or more of the following items:
		1. Item 14, Limited Purpose
		2. Item 16, Required Task
		3. Item 17, Charging third parties
		4. Item 23, Outsourcing IT
		5. Item 24, Security Protocols
		6. Item 25, Attestation of last audit
		7. Item 26, Exception to Log Form
	4. Applicant should also submit supplemental pages for any other item where additional explanation is warranted. For instance, some DC may require supplemental pages for Item 16.
	5. Once the draft is complete, email it to DEContracts@twc.texas.gov. A TWC Contract Manager will review the draft and provide feedback. Please allow up to three business days to receive the assigned Contract Manager's contact information. Once the applicant has been assigned a CM, the applicant can direct any questions regarding the draft RSP to them. Applicant should collaborate with the CM to revise the draft based on the CM’s feedback.
	6. When the applicant has addressed all the issues raised by the CM, the RSP will be considered complete. At that point, applicant should sign and date the final version of the RSP and submit it to assigned CM.
	7. The RSP serves as the applicant’s application for an EDE contract. Upon finalization, signing, and submission of the RSP, TWC will initiate the application processing procedure.

### **3.3.3 Online RSP Instructions**

1. **Exact Legal Name (Item 1)**
	1. The EDE contract will be between TWC and applicant. Provide the name of the applicant who will sign the contract. This must be the same entity as the employer of the people who will access and use the TWC Data. This is critically important. If the applicant names an entity other than the employer; the application will be denied. By law, only employees of the applicant in Item 1 can access and use the TWC Data.
2. **Tax ID (Item 2)**
	1. TWC is not able to issue a contract without a Tax ID number. It is a required field, as are all items in the application. Applicant may need to contact the applicant’s finance or legal department to get the applicant’s Tax ID number.
3. **DC’s Address (Items 3-5)**
	1. Provide the physical address of the DC.
4. **Seeking Offline Access (Item 6)**
	1. Select the RSP for the type of data access needed. Refer to Section 2.2 above to differentiate between Offline and Online access.
5. **List of Contracts with TWC (Items 7-8)**
	1. Items 7 and 8 request information regarding any existing legal agreements the applicant has with TWC. It is essential to provide accurate contract numbers, as these are unique identifiers used for all TWC contract-related communications. Please list all EDE contract numbers in Item 7 and any other relevant TWC contract numbers in Item 8. Providing this information is crucial for TWC to determine the most appropriate and secure approach for documenting data sharing arrangements with the applicant.
6. **Contract’s Initial Term (Item 9)**
	1. TWC generally prefers contracts with a five-year term, aligning with the maximum duration permitted by the state. However, TWC recognizes that not all applicants have the budgetary capacity to commit to a five-year agreement. Indicate the desired contract duration in the designated section of the application.
7. **Start Date (Item 10)**
	1. When selecting the checkboxes, specify if the applicant requests the EDE contract to align with the federal fiscal year or another annual cycle relevant to the applicant. Furthermore, if applying for the contract during the middle of the preferred cycle, please detail the preferred method for aligning future contract years. For example, indicate the initial contract year to be less than twelve (12) months to facilitate alignment with the desired annual cycle in subsequent years.
8. **Type of Entity (Item 11)**
	1. Please select only one organizational type. While any organization is eligible to apply for an EDE contract, please be aware that TWC rarely approves RSPs submitted by for-profit or non-profit entities. Most EDE contracts are awarded to governmental entities. Therefore, carefully consider this information when selecting the appropriate option in Item 11.
9. **Contract Authority and Mission of Recipient (Items 12-13)**
	1. Provide a statutory citation demonstrating the applicant’s legal authority to enter into contractual agreements. Some legal entities possess limited or no authority to execute contracts, and all entities operate under a statute that defines their contractual powers, if any. Applicant may need to consult with applicant’s legal department to obtain the appropriate legal citation to fulfill this requirement.
	2. For Item 13, select only one (1).
10. **Limited Purpose (Item 14)**
	1. Federal law (Rule 603) mandates that any use of TWC data requires prior approval. Securing an EDE contract grants the applicant authorization to utilize TWC data solely for the specific purposes and tasks documented and approved within the RSP.
	2. Approval for specific data uses is not guaranteed for all DCs. The only way to determine if a particular intended use will be approved in the requested circumstances is to explicitly request it in response to Item 14, enabling TWC to thoroughly evaluate the request. To determine the precise purposes and uses of TWC data within the applicant’s organization, consult with the individuals who manage or lead the employees utilizing this data.
	3. A critical aspect of TWC's ongoing monitoring is ensuring that TWC data is not used for any purpose that was not disclosed and explicitly approved. Improper or unauthorized data use will trigger TWC's right to legal remedies, including potential termination of the data sharing contract.
11. **Withdrawn Uses (Item 15)**
	1. If this is the initial draft of the RSP, please select the "no" box in Item 15. Should the assigned CM subsequently inform the applicant that one or more of the uses outlined in the response to Item 14 are not approved, take the following actions in the next draft submission: 1) deselect the disallowed purpose in Item 14, 2) select the "yes" box in Item 15, and 3) provide a comprehensive list of all purposes that were requested but not approved by the CM.
12. **Required Task (Item 16)**
	1. If the applicant is legally obligated, through a state or federal statute or other regulatory authority, to perform a task that necessitates access to TWC's data, provide a specific citation to the relevant statute, regulation, or authority. Additionally, provide a detailed description of the task that the applicant is mandated to complete. Providing this information is crucial for demonstrating the legal basis for the data request.
13. **Charging a Fee to Third Parties (Item 17)**
	1. Regarding the use of TWC Data for determining eligibility for public assistance or public services, please carefully consider the following:
		1. If the applicant will not be utilizing TWC Data in the process of determining eligibility for public assistance or public services, select the first "no" box and proceed to the next section.
		2. If the applicant is a public hospital, public health facility, or determines eligibility for any program or benefit other than public health, and bills patients or beneficiaries for any services or benefits, even in specific situations, select "yes" and attach the required supplemental pages. This encompasses any billing or charging to the individual receiving benefits or participating in the program, financial guarantors, family members, or residents in the individual's household. If uncertain about whether or how often individuals are charged in connection with eligibility determinations, select "yes" and attach the supplemental pages.
		3. If applicant selects "yes," please copy and paste the following statement (including the italics and underlining) at the end of your supplemental pages: *Accessing, viewing, or using TWC data must be for the sole purpose of making an eligibility determination as described above. No one will use TWC data for any other purpose, task, or program. In particular, TWC’s data must never be used for collections, credit, credit worthiness or accounts payable functions.*
		4. To ascertain whether the applicant engages in any billing or charging practices, it may be necessary to consult with applicant’s finance department or the individuals who manage employees who utilize TWC Data.
14. **Information Requested (Item 18)**
	1. Specify the types of data searches that are required for the applicant’s employees to conduct within the TWC system. To ensure accurate account configuration, it may be necessary to consult with the individual who oversees the employees that utilize TWC's data resources to determine the specific search functionalities needed. TWC will configure the account accordingly once we receive this information.
15. **Number of Individuals with Login credentials (Item 19)**
	1. Indicate in Item 19 the number of employees who require access to the TWC web portal. To ensure accurate provisioning and alignment with federal regulations (Rule 603), TWC must minimize access to TWC data to the least amount necessary. Provide a user range (e.g., 1-10, 11-25) that encompasses the actual number of employees requiring access. Acknowledge the agreement to minimize credentials issued by selecting "yes" or "no." Note that TWC typically approves requests for up to 25 users. If the operational needs necessitate access for more than 25 users, provide a detailed justification in the designated section of Item 19. Finally, be aware that the response in Item 19 will influence the invoice amount. Important: TWC does not accept POs under the EDE contract, as it is an inter-governmental cooperation arrangement, and TWC is recouping costs associated with the agreement. Consult with the individual overseeing TWC data usage within the applicant’s organization for precise user count details.
16. **Redisclosure (Item 20)**
	1. Item 20 specifically pertains to the process of managing log-in credentials for accessing the TWC data portal. Detail the applicant’s procedures for granting, revoking, and monitoring access rights to ensure data security.
17. **Part A and Part of Redisclosure (Item 21)**
	1. This section pertains to documenting various aspects of how the applicant manages and handles TWC data within the applicant. Part A inquires whether individuals other than direct, permanent employees will be *using* the data. Part B asks whether individuals other than direct, permanent employees will have *access* to the data.
	2. If either of these processes involves non-employees, applicants are required to provide a detailed description by selecting the appropriate checkboxes and providing additional information. TWC approval is mandatory for any such arrangement. If approved, the applicant must acknowledge the acknowledgement box on the RSP and fulfill the associated obligations. The applicant may need to consult with the HR department, IT department, or the individuals who manage employees who use TWC's data to accurately complete this section.
18. **Background Checks (Item 22)**
	1. This section requests information regarding the applicant’s use of background checks to safeguard TWC data. Describe the current background check practices and how they contribute to protecting the confidentiality and integrity of the data. To provide a complete and accurate response, the applicant may need to consult with the HR department or the individuals who manage employees who use TWC's data.
19. **Outsourcing IT Tasks (Item 23)**
	1. This section addresses the use of outsourcing in the applicant’s IT infrastructure. For the purpose of this document, "outsourcing" refers to situations where individuals performing IT work for the applicant are not employees of the entity named in Item 1. "IT" encompasses all aspects of Information Technology, including the installation, security, and maintenance of the hardware and software.
	2. If the applicant exclusively utilizes employees for all IT-related tasks, please select the "no" box. However, if any part of the IT system is managed by non-employees, select "yes" and provide comprehensive details, attaching supplemental pages as needed to fully explain the arrangement. Applicants may need to consult with the IT department, Chief Information Security Officer, HR department, or legal department to accurately complete this section.
20. **Data Security Protocols (Item 24)**
	1. Security protocols outline the specifications and detailed guidelines for safeguarding all aspects of applicant’s IT system. These protocols establish standards for areas such as firewalls, password management, physical access control, electronic access control, and procedures for handling security breaches.
	2. Item 24 assesses the current state of the applicant’s IT system protection. For Item 24A, indicate whether the applicant has formally committed to a recognized set of security protocols. If so, please specify which protocol set has been adopted.
	3. For Item 24B, if the applicant has formally adopted a set of security protocols but has not yet fully implemented and achieved compliance, attach supplemental pages describing the specific steps taken and the timeline for achieving full implementation and compliance.
	4. If, in Item 24A, applicant indicated the applicant has not adopted any recognized set of security protocols, then in Item 24B, select the "no" box and attach supplemental pages detailing the improvements or upgrades planned to be implemented within the next six (6) to twelve (12) months.
	5. Applicants may need to consult with the applicant’s auditor, risk manager, Chief Information Security Officer, IT department, or legal department to accurately complete this section.
21. **Assessing Security (Item 25)**
	1. Item 25 requests fundamental information regarding the frequency and methodology employed to assess and confirm that the applicant adheres to the security protocols it has adopted.
	2. Please note that an "attestation" is a distinct document, typically a concise, self-contained record (often one page or less) confirming that a security assessment has been conducted. An attestation is *not* a copy of the assessment results themselves. **Do not submit copies of your assessment results to TWC.**
	3. Applicant may need to consult with applicant’s auditor, risk manager, Chief Information Security Officer, IT department, or legal department to accurately complete this section.
22. **Exception to Standard Form (Item 26)**
	1. The Quarterly Self-Assessment Report (QSAR) is a comprehensive document that must be submitted to TWC every ninety (90) days, detailing the proactive measures the applicant takes to ensure the proper handling of TWC data. The QSAR requires the submission of specific forms, including a usage log, which the applicant is required to maintain using the TWC-provided template. Use of the TWC-provided log form is mandatory.
	2. If the applicant utilizes case management software or another integrated system to track each instance of accessing the TWC web portal and wish to submit reports generated from that software in lieu of the mandatory log form, please indicate that preference in Item 26 and attach supplemental pages showcasing the format and content of applicant’s proposed alternative report.
	3. Ensure that reports do not contain any Personally Identifiable Information (PII) and do not include any data that could enable a third party to ascertain the identity of any search subject (individual or employer). Reports must contain sufficient information to allow the applicant to 1) readily retrieve the case file containing the TWC Data accessed during that search if requested by TWC, and 2) enable TWC to identify the date and time of the search for cross-referencing with our internal records.
23. **Disposing of Data (Item 27)**
	1. Federal law (Rule 603) mandates the proper and secure disposal of all TWC data. The Certificate of Destruction for Contractors and Vendors, which outlines the requirements for data disposal, can be found in [Section V (Data Disposal)](#_Section_V_Data) of this document. Please consult this document for detailed instructions on compliant data disposal procedures.
24. **Data Encryption (Item 28)**
	1. Select type of data encryption used to protect TWC data at rest.
	2. Applicants may need to contact the IT department for this information.
25. **Compliance Liaison (Items 29-31)**
	1. TWC approval is required for applicant’s designated CL. The CL must be an executive or senior manager within the entity identified in Item 1, possessing the authority to address and rectify issues raised by TWC. While the CL can delegate specific tasks, they must serve as the primary point of communication with TWC when requested.
	2. It is important to distinguish between the CL and the POC. The POC, often an administrative or clerical staff member designated in Item 35, typically manages the day-to-day paperwork and contract administration for the DC. While most TWC communications will be directed to the POC, the CL will also be copied on certain messages, including formal legal notices.
	3. The CL will be contacted and expected to address situations of a more serious nature, requiring the attention of a higher authority capable of making policy-level decisions to ensure ongoing or restored compliance with the conditions and restrictions outlined in the EDE contract, as well as adherence to federal law.
	4. When selecting applicant’s CL nominee, carefully consider the following questions:
		1. Is the individual an executive or upper-level manager within the applicant’s organization?
		2. Does the individual possess the authority to assign tasks to staff and require operational changes within the applicant’s organization?
		3. Do the individual's role and title align with these responsibilities?
		4. Are there other factors demonstrating the individual's suitability for the CL role to TWC's satisfaction?
		5. In the event of a violation of 20 CFR 603, can the individual immediately implement corrective action?
		6. If TWC were to conduct an on-site review of the performance under the EDE contract, would the individual be able to require staff within the applicant’s organization to provide TWC with all necessary access and information?
		7. If the applicant were at risk of losing its EDE contract due to a breach of contract conditions or restrictions, would this individual have the authority to implement preventative measures to avoid termination?
		8. As a critical example, termination will occur if the POC fails to submit the QSAR on time or fails to complete it correctly.
26. **Contact Information (Items 32-56)**
	1. Provide the required information for the CL, POC, Alternate POC, Signatory (authorized representative signing on behalf of the entity named in Item 1), Data Technology contact, and the designated recipient for TWC invoices.
	2. As a reminder, the RSP states: "If the application leads to a contract, applicant agrees to provide written notice to TWC of any changes to the responses contained in this RSP immediately but no later than three (3) calendar days from the date of change. Email changes to DEcontracts@twc.texas.gov." It is crucial to maintain accurate and up-to-date contact information with TWC throughout the duration of the contract.
27. **Invoices (Item 52)**
	1. Provide the contact information for the individual responsible for receiving invoices from TWC. TWC will send invoices directly to this contact. It is imperative to understand that the applicant should not send a PO for this transaction. This is not a procurement, and TWC is not acting as a vendor selling data, subscriptions, or any other goods or services. An EDE contract constitutes a cooperation agreement, and TWC is obligated under federal law (Rule 603) to recover costs associated with sharing TWC Data.
28. **Signature**
	1. The "attestation" section is located directly above the signature line. By signing the RSP, the applicant is agreeing to and attesting to the accuracy of all responses provided within the document, as well as specifically acknowledging the points outlined in the attestation itself.
	2. Given that applicant’s responses in the RSP will be legally binding upon the entity named in Item 1, applicant may wish to have applicant’s legal counsel review the draft RSP responses before submitting them to TWC.
	3. For many DCs, particularly first-time applicants, it may be prudent to defer signing the draft RSP. While it is not incorrect to sign the draft, please be aware that it is likely applicant will need to obtain a new signature on a revised version following feedback from TWC.

**Important:** The name and title provided in the signature block (and the signed name itself) must precisely match the information provided in Items 44 and 45.

1. **Steps to Complete your RSP**
	1. To complete the application process, fill out the RSP form using only the form itself and these instructions. Provide applicant’s best possible response for each and every item, ensuring that no items are left blank.
	2. Confirm that applicant’s designated CL has reviewed and approved all draft answers, as indicated in Item 30.
	3. Please ensure all necessary supplemental pages are attached. Depending on the applicant’s specific circumstances, applicant may have no supplemental pages, or may require them for one or more of the following items:
		1. Item 14, Limited Purpose
		2. Item 16, Required Task
		3. Item 17, Charging third parties
		4. Item 23, Outsourcing IT
		5. Item 24, Security Protocols
		6. Item 25, Attestation of last audit
		7. Item 26, Exception to Log Form
	4. Applicant should submit supplemental pages for any other item where additional explanation is warranted. For instance, some DCs may require supplemental pages for Item 16.
	5. Once the draft is complete, email it to DEContracts@twc.texas.gov. A TWC Contract Manager will review applicant’s draft and provide feedback. Please allow up to three business days to receive the CM's contact information. Once you have been assigned a CM, applicant can direct any questions regarding the draft RSP to them. Please collaborate with the CM to revise the draft based on their feedback.
	6. When the applicant has addressed all the issues raised by the CM, the RSP will be considered complete. At that point, applicant should sign and date the final version of the RSP and submit it to the assigned CM.
	7. The RSP serves as the applicant’s application for an EDE contract. Upon finalization, signing, and submission of applicant’s RSP, TWC will initiate the application processing procedure.

# Section IV Quarterly Self-Assessment (QSAR)

## 4.1 Online QSAR Instructions

1. **Complete Header Information**
2. Fill in the blanks
	1. Contract Number
	2. Applicant Name
	3. Name of Person Submitting Report
	4. Name of Compliance Officer
	5. Period Covered
		* 1. Enter the Year
			2. Select the Month of Submission (Jan, Apr, Jul, Oct)
		1. **Compliance Questions**
3. For each of the following Sections check Yes or No, and if necessary, complete any supplemental pages and attach them to the QSAR.
	* 1. **Detailed Layout Overview**
4. If the contact details for the points of contact listed in Exhibit 1 – Request and Safeguard Plan have changed, a formal letter requesting the update must be submitted. This is required in order to accept a signature on the QSAR form.
	* 1. **Daily User Activity**
5. Please confirm whether the Recipient has attached the Daily User Activity list to the QSAR form. The log can be located at https://www.twc.texas.gov/agency/contract-opportunities
	* 1. **Quarterly Active Users List**
6. Please confirm whether the Recipient has attached the Quarterly Active Users List to the QSAR form. The log can be located at https://www.twc.texas.gov/agency/contract-opportunities
	* 1. **User Logs**
7. Please confirm the user logs submitted to the TWC along with the QSAR form do not include any Sensitive Personally Identifiable Information (PII).
	* 1. **Disclosed TWC Information**
8. Please confirm that any TWC information received was used only for the specific purpose authorized by law and outlined in Exhibit 1 (RSP) of the contract. If the use is not listed or approved in Exhibit 1, it must be marked “No.”
	* 1. **Physical Security**
9. Please confirm hard copies are physically secure from unauthorized access.
	* 1. **Confidentiality Training**
10. Please confirm that all personnel have received training on 20 C.F.R. § 603.9 and are aware of the state penalties associated with unauthorized disclosure of confidential information.
	* 1. **Confidentiality Requirements**
11. Confirm that all personnel with access to disclosed TWC information have been instructed on the confidentiality requirements outlined in 20 C.F.R. § 603.9 and have been informed of the applicable state penalties for unauthorized disclosure.
	* 1. **Staff Responsibilities Reminder**
12. Confirm that Recipient’s staff have been reminded of the policy prohibiting access to coworker information without proper authorization.
	* 1. **Security Safeguards**
13. Confirm Recipient established and maintained adequate data security safeguards.
	* 1. **Data Disposal**
14. Confirm the Recipient has disposed of TWC data obtained through an Online Contract in accordance with their data retention protocol. If the retention protocol is being followed, there is no need to apply for an extension to the three-year data retention limit.
	* 1. **Data Retention**
15. Confirm no personal identifiers are retained beyond the limited purpose or beyond the three years.
	* 1. **Audit Compliance**
16. Confirm the Recipient maintained a system sufficient to allow an audit of compliance with the requirements of 20 C.F.R § 603.9 and the TWC Contract.
	* 1. **New or Supplemental Use of TWC Data**
17. Confirm whether the recipient uses TWC data for any supplemental purpose by checking “no” if no such use exists. If the Recipient does

engage in supplemental use, a separate document outlining the new purpose must be attached to the QSAR. This will require TWC approval and an amendment to the contract to formally incorporate the new usage.

* + 1. **TWC Annual Security Training**
1. Confirm whether all users have completed the required TWC Security Training within the past twelve (12) months, in accordance with the annual training requirement. If any user has not completed the training, their access will be revoked until the training is completed and the documentation is submitted to EAGLE SUPPORT.
	* 1. **User Violation**
2. Confirm if the Recipient has notified TWC of any suspected or confirmed user violation of confidentiality and security provisions within twenty-four (24) hours of discovery and taken appropriate action.
	* 1. **Automated Systems**
3. Confirm the Recipient used any automated systems, macros, or software to make multiple inquiries of TWC’s computer-store files.
	* 1. **Breach or Unauthorized Access**
4. Confirm that there have been no breaches or unauthorized access involving the data received from TWC.
	* 1. **Yes, to Question 17**
5. Confirm whether the recipient purchased identity theft protection for the individuals affected by the incident.
	* 1. **Controlled Access Usage**
6. Confirm that all TWC data is stored and used exclusively within secure, access-controlled environment.
	* 1. **Data Re-Disclosure**
7. Confirm whether, if applicable, there is express contract language permitting this arrangement and that all contractors meet the required training and security standards.
	* 1. **Certification and Signature**
8. Recipient’s Point of Contact or CL completes the required fields, including their signature, the date of completion, and their printed name along with title.
	* 1. **Submit the Completed Form**
9. Once the QSAR and all accompanying attachments are complete, submit them via email to: SelfAssessmentReports@twc.texas.gov.

## 4.2 Offline QSAR Instructions

1. Complete Header Information

* 1. Fill in the blanks at the top of the form:
		1. Contract Number (29##EDE###)
		2. Recipient Name
		3. Name of Person Submitting Report
		4. Name of Compliance Officer
		5. Period Covered
			1. Enter the Year
			2. Select the Month of Submission (Jan, Apr, Jul, Oct)

2. Compliance Questions

For each of the following sections check Yes or No, and if necessary, complete any supplemental pages and attach them to the QSAR.

3. Detailed Layout Overview

a. Change in Contact Information

If the contact details for the points of contact listed in the RSP have changed, a formal letter requesting the update must be submitted. This is required in order to accept a signature on the Quarterly Self-Assessment form.

* 1. Daily User Activity

Confirm whether the recipient has attached the Daily User Activity list to the QSAR form. The log can be located at <https://www.twc.texas.gov/agency/contract-opportunities>.

* 1. Disclosed TWC Information

Confirm any TWC information Recipient received was used only for the specific purpose authorized by law and outlined in Exhibit 1 of the contract (RSP). If the use is not listed or approved in Exhibit 1, it must be marked “No.”

  *d. Physical Security*

Confirm hard copies are physically secure from unauthorized access.

* + - 1. Security Precautions for Stored TWC Data

Confirm Recipient has implemented appropriate access controls for TWC information stored in the systems.

* + - 1. Confidentiality Requirements

Confirm that all personnel with access to disclosed TWC information have been instructed on the confidentiality requirements outlined in 20 C.F.R. § 603.9 and have been informed of the applicable state penalties for unauthorized disclosure.

* + - 1. Staff Responsibilities Reminder

Confirm Recipient’s staff have been reminded of the policy prohibiting access to coworker information without proper authorization.

* + - 1. Security Safeguards

Confirm Recipient established and maintained adequate data security safeguards.

* + - 1. Data Disposal

Confirm Recipient has disposed of TWC data obtained through an Offline Contract in accordance with their data retention protocol. If the retention protocol is being followed, there is no need to apply for an extension to the three-year data retention limit.

* + - 1. Data Retention

Confirm no personal identifiers are retained beyond the limited purpose or beyond the three years.

* + - 1. Audit Compliance

Confirm Recipient maintained a system sufficient to allow an audit of compliance with the requirements of 20 C.F.R § 603.9 and the TWC Contract.

* + - 1. Encryption Requirements

Confirm encryption standards were met: FIPS 140-2, 256-bit AES.

* + - 1. New or Supplemental Use of TWC Data

Confirm whether Recipient uses TWC data for any supplemental purpose by checking “no” if no such use exists. If Recipient does engage in supplemental use, a separate document outlining the new purpose must be attached to the QSAR. This will require TWC approval and an amendment to the contract to formally incorporate the new usage.

* + - 1. User Violation

Confirm if Recipient has notified TWC of any suspected or confirmed user violation of confidentiality and security provisions within twenty-four (24) hours of discovery and taken appropriate action.

* + - 1. Quarterly Data Submission

Confirm Recipient submitted a list of data requests and data received to the TWC POC for the prior quarters (Quarterly Filing Dates: January 15, April 15, July 15, and October 15).

* + - 1. Breach or Unauthorized Access

Confirm there have been no breaches or unauthorized access involving the data received from TWC.

* + - 1. Yes, to Question 17

Confirm whether Recipient purchased identity theft protection for the individuals affected by the incident.

* + - 1. Controlled Access Usage

Confirm that all TWC data is stored and used exclusively within secure, access-controlled environment.

* + - 1. Data Re-Disclosure

Confirm whether, if applicable, there is express contract language permitting this arrangement and all contractors meet the required training and security standards.

* + - 1. Certification and Signature

Recipient’s POC or CL completed the required fields, including their signature, the date of completion, and their printed name along with title.

* + - 1. Submit the Completed Form

Once the QSAR and all accompanying attachments are complete, submit them via email to: SelfAssessmentReports@twc.texas.gov.

# Section V Data Disposal

This section outlines the conditions under which the DC is released from the requirements of Code of Federal Regulations (CFR), Rule 603 and when TWC is no longer obligated to monitor compliance. As specified in § 603.9 (b)(1)(vi), TWC requires that the DC must dispose of UI information once the purpose for which the information was disclosed has been fulfilled. Disposal is defined to include the deletion of personal identifiers as an alternative to the complete destruction of the data.

## 5.1 Data Destruction and De-Identification Requirements

**Certificate of Destruction**

DCs must submit a Certificate of Destruction Form for each instance of a data destruction.

**De-Identification of Data**

If the DC elects to de-identify data they will need to provide a detailed explanation of the process, including when and how it was completed. The steps taken to the de-identify the data must be documented, and a copy of this documentation must be submitted to TWC.

The DC is responsible for maintaining records on how and where documentation related to de-identified data is stored.

##  Compliance with Standards

The DC must confirm whether the de-identification process meets the standards and requirements outlined in [National Institute of Standards and Technology, Special Publication (NIST-SP) 800-88 Revision 1.](https://doi.org/10.6028/NIST.SP.800-88r1) The DC must disclose whether any TWC confidential data remains in their possession after the de-identification process.

The DC must notify TWC of any updates or changes related to:

* Firewall configurations
* Encryption measures
* Security policies

The following information must be provided to TWC:

* Date of the most recent internal/external audit
* Copy of the most recent written attestation of the last internal/external audit