DATA SHARING AGREEMENT
BETWEEN
WASHINGTON STATE
EMPLOYMENT SECURITY DEPARTMENT
AND
CITY OF TACOMA

1. INTRODUCTION

This Agreement is made and entered into by and between the Washington State Employment Security Department (hereinafter "ESD") and the City of Tacoma (hereinafter called "COT"), pursuant to authority granted by the Revised Code of Washington (RCW) in RCW 39.34, RCW 50.13 and RCW 50.38 , other relevant federal statutes, and related regulations.

2. DEFINITIONS

"Authorized user" means any COT employee approved by both parties to receive confidential Unemployment Insurance Data (UI Data) pursuant to this Agreement.

"Data Security" means defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This applies regardless of the form the Data may take (electronic, physical, etc.).

"Data Security Breach" means unauthorized acquisition of Data that compromises the security, confidentiality, or integrity of Personal Information maintained by the person or business. "Breach of the security of the system" and "Personal Information" are defined in RCW 19.255.005.

"Data Security Requirements" means the minimum requirements COT must comply with to ensure Data Security.

"Managed File Transfer" means a method that protects the Data in transit to prevent viewing and manipulation by another.

"Permissible Use" means only those uses authorized in this Agreement and as specifically defined herein.

"UI Data" means confidential unemployment insurance information in the record of ESD collected from employers and individuals for the administration of the state unemployment insurance program as set forth in the federal law (20 CFR 603) and state statutes (RCW 50.13 and RCW 50.38). "UI Data" is classified as Category 4 data according to WaTech policy SEC-08-01-S Data Classification Standard.

3. PURPOSE

The purpose of this Agreement is to:

3.1 Set out the terms and conditions under which ESD will share the UI Data with COT set forth in the federal law (20 CFR 603) and state statutes (RCW 39.34 and RCW 50.13).

3.2 Define the safeguards against unauthorized use or disclosure of UI Data by COT.

4. STATEMENT(S) OF WORK

4.1 ESD will share data with COT based on the specifications of each numbered Statement of Work, which shall be incorporated into this agreement by reference as Exhibit A.

4.2 Each numbered Statement of Work shall specifically identify the type and category of data requested, the purpose for which it will be used ("Permissible Use"), the legal authority for the disclosure by ESD to COT, and each Statement of Work will be authorized and signed by both parties.

5. TERMS AND CONDITIONS

All rights and obligations of the parties to this Agreement shall be subject to and governed by the terms and conditions contained in this Agreement.

6. PERIOD OF PERFORMANCE

6.1 Subject to its other provisions, the period of performance of this Agreement shall start on the date of execution and end on 30 November 2028, unless terminated sooner as provided herein. The parties may extend the Agreement for up to three additional one-year terms by mutual written consent signed by both parties. The total duration of this Agreement, including extensions, will not exceed six years.

6.2 Each Statement of Work, incorporated into this Agreement as Exhibit A, shall terminate on the date stated in the PERIOD OF PERFORMANCE clause of the respective Statement of Work, unless amended or modified as provided herein. No Statement of Work shall extend beyond the end date of this Agreement.

7. CONSIDERATION

COT agrees to adhere to the requirements of the Consideration clause stated in each of the numbered Statements of Work incorporated into this agreement as Exhibit A.

8. AGREEMENT MANAGEMENT

COT staff member responsible for the management of this Agreement is:	**ESD staff member responsible for the management of this Agreement is:**
Kris Oldenburg	Madeline Veria-Bogacz

Audit and Compliance Manager
747 Market Street
Tacoma, WA 98402
Phone: 253-573-2442
Email address:
koldenburg@cityoftacoma.org

Data Sharing Manager
212 Maple Park Ave SE
Olympia, WA 98501
Phone: 360-763-2340
Email address: madeline.veria-bogacz@esd.wa.gov

ESD's Agreement Manager shall monitor the performance and compliance of this Agreement. ESD's Agreement Manager shall be responsible for the review and acceptance of the COT performance, deliverables, and reports as well as compliance with the data security permissible use requirements and COT's Audit requirements. The Agreement Managers will be the main contacts for any questions about the Agreement.

9. DATA DISPOSAL; PERMISSIBLE USE; BREACH

COT agrees to the following limitations on the use of the information provided by ESD:

9.1 Data Disposal:

Unless a more immediate disposal requirement is set forth in this Agreement, COT, upon completion of each applicable Statement of Work or upon termination of this Agreement, shall erase, destroy, and render unrecoverable all ESD UI Data and certify to the Agreements Manager in writing that these actions have been completed within thirty (30) days of the completion of the Statement of Work or termination as more specifically described in Section 27.3 of this Agreement. Disposal includes deletion of personal identifiers in lieu of destruction.

9.1.1 All ESD UI Data including individual records, lists or screen prints not admitted as exhibits will be purged from all COT systems, servers, and computers as soon as no longer needed (NIST Standard: 800-88 Guidelines for Media Sanitization).

9.1.2 All hard copy UI Data including paper or compact disc copies will be shredded to a size no larger than 1/8 by 1 1/8-inch size in a crosscut shredder or deposited into a locked shredder bin to be shredded by a company contractually bound to maintain confidentiality of materials being shredded.

9.1.3 The COT's Statement of Work Manager shall inform the ESD Statement of Work Manager in writing as to the method and frequency of UI Data use and destruction.

9.2 Permissible Use: The information provided by ESD to the COT shall be used and accessed only for the permissible uses described in the applicable numbered Statement(s) of Work.

9.3 **Confidentiality:** COT shall protect the confidentiality of the UI Data as required by the laws cited in this Agreement including specifically 20 CFR 603, RCW 39.34 and RCW 50.13 in connection with COT's use of the UI Data as provided under this Agreement.

9.4 **Data Breach**: If COT has reason to believe that there has been a UI Data security breach COT and ESD must follow the requirements in RCW 42.56.590. COT will, as soon as is practical but no later than 24 hours give ESD notice and take actions to eliminate the cause of the breach. COT shall provide detailed information, including the nature of the unauthorized activity, names of individuals involved, work locations where the incident occurred, and the action taken by COT in sufficient detail to enable ESD to conduct its own investigation if necessary.

To the extent the ESD deems warranted, in its sole discretion, COT may be required by ESD to provide notice to individuals whose personal information may have been improperly accessed or disclosed, and to cover the costs incurred by ESD or the Department of Enterprise Services (DES) in providing notice and other related services to those individuals.

10. PHYSICAL SAFEGUARDS AND SECURITY

COT agrees to the following minimum safeguards for the UI Data provided by ESD as follows:

10.1 Access to the UI Data provided by ESD will be restricted to only those COT authorized personnel who need it to perform their official duties, who have been advised of the security and permissible use requirements, and have signed the Nondisclosure Agreement attached hereto as Exhibit B. COT will restrict access to data based on principles of least privileged and enforce separation of duties to reduce risk of misuse of access.

10.2 The UI Data will be stored in areas that are safe from access by unauthorized persons during regular business hours as well as non-business hours or when not in use. Data stored in rest or data in transit must be encrypted using NIST Standard FIPS PUB 140-3 or higher encryption standards and configured according to baselines (CIS Level 1 or similar) that limits unnecessary services and permissions.

10.3 The UI Data will be protected in a manner that prevents unauthorized persons from retrieving the UI Data by means of computer, remote terminal, or other means, and where applicable the system that holds shared UI data should be segregated on the network.

10.4 COT shall take precautions to ensure that only authorized personnel are given access to UI Data files. Electronic access is to be authorized using multifactor authentication and hardened passwords that are changed at least every 90 days.

10.5 When applicable COT shall furnish encryption and decryption software compatible with ESD's software to ensure security and confidentiality.

10.6 COT will have up-to-date anti-virus software installed and shall be diligent in the timely updating of this software. This includes the timely installation of security patches for all information technology assets, hosts, and networks that process ESD confidential information. Technology assets will undergo regular vulnerability scanning and any weakness identified should be remediated immediately. COT will do regular risk assessment and implement continuous monitoring to detect any potential security vulnerabilities.

10.7 COT shall establish an audit trail that logs the activities of authorized users. COT shall grant ESD access to the audit trail upon request for investigative and compliance monitoring purposes. COT will review logs regularly and implement alerting for any unauthorized attempts to access or modify data.

10.8 COT shall instruct all authorized personnel regarding the confidential nature of the UI Data, the requirements of the LIMITATION ON ACCESS AND USE and PHYSICAL SAFEGUARDS clauses of this Agreement, and the sanctions specified in RCW 50.13.110 and other federal and state laws against unauthorized disclosure of UI Data covered by this Agreement.

10.9 COT employees shall only access the ESD data provided through hardware owned by COT which is located on COT premises or secured through appropriate VPN or similar security protection. UI Data will not be accessed via the following devices, including but not limited to cell phones, tablets, or at public wireless hotspots.

10.10 The COT Contract Manager will sign an acknowledgment that all personnel having access to the disclosed information have been instructed in accordance with Section 10.9 and will adhere to ESD's confidentiality requirements and procedures and agreeing to report any infraction to ESD fully and promptly.

11. REDISCLOSURE OF INFORMATION

11.1 Redisclosure of confidential UI Data received from ESD is prohibited by RCW 50.13.110 and 20 CFR 603.9(c) unless there is written authorization by ESD for the official purpose for which the UI Data was originally requested, and the requirements of 20 CFR 603.9(c) otherwise have been met. As part of approval of the redisclosure, the COT remains liable for the data after redisclosure and shall ensure the party that obtains the confidential UI Data is compliant with the terms and conditions of this Data Sharing Agreement.

11.2 Redisclosure of ESD UI Data is authorized for judicial, formal administrative, or discovery proceedings only by subpoena pursuant to RCW 50.13.070.

11.3 Parties or individuals redisclosing confidential UI Data in violation of RCW 50.13.110 are subject to civil penalty. ESD may pursue criminal charges against individuals engaged in unauthorized redisclosure of Unemployment Insurance data.

11.4 COT agrees to reimburse ESD for all costs associated with the criminal referral and conviction of any COT employee engaged in any form of unauthorized redisclosure of Unemployment Insurance data.

12. EXPORT

COT agrees not to export, report, or transfer, directly or indirectly, UI Data, or any products utilizing such data, in violation of United States export laws or regulations. Without limiting the foregoing, COT agrees that (a) it is not, and is not acting on behalf of, any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States or other applicable government body has prohibited export transactions (e.g., Iran, North Korea, etc.); (b) is not, and is not acting on behalf of, any person or entity listed on a relevant list of persons to whom export is prohibited (e.g., the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, the U.S. Commerce Department Denied Persons List or Entity List, etc.); and (c) it will not use any UI Data for, and will not permit any UI Data to be used for, any purpose prohibited by applicable law.

13. DATA CLASSIFICATION

According to WaTech policy SEC-08-01-S Data Classification Standard, Section 1, agencies must classify data into categories based on its sensitivity and handling requirements. Agency data classifications must translate to or include the following classification categories:

i) **Category 1** – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

ii) **Category 2** – Sensitive Information

Sensitive information is not specifically protected from disclosure by law but is for official use only. Sensitive information is generally not released to the public unless specifically requested.

iii) **Category 3** – Confidential Information

A. Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

B. Personal information as defined in RCW 42.56.590 and RCW 19.255.010.

C. Information about public employees as defined in RCW 42.56.250.

D. Lists of individuals for commercial purposes as defined in RCW 42.56.070(8).

E. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

iv) **Category 4** – Confidential Information Requiring Special Handling

A. Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

B. Especially strict handling requirements are dictated, such as by statutes, regulations, agreements, or other external compliance mandates.

C. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

The UI Data provided to COT under this Agreement is classified as **Category 4 – Confidential Information Requiring Special Handling.**

14. DATA REPROCESSING

COT shall have the right to reformat and/or reprocess the UI Data using software or other technology, and the reprocessed UI Data will be owned by ESD; provided that such reprocessed UI Data shall be subject to the same restrictions regarding confidentiality, use, disclosure, and transfer as the UI Data covered hereby, and so marked to indicate such restrictions.

15. NO GUARANTEE OF ACCURACY

ESD does not guarantee the accuracy of the data provided.

16. TERMINATION OF ACCESS

16.1 ESD may at its sole discretion disqualify any individual authorized by COT from gaining access to UI Data. Notice of termination of access to UI Data will be by written notice and become effective upon receipt by COT. Termination of access of one individual by ESD does not affect other individuals authorized under this Agreement.

16.2 ESD Agreement Manager identified in Section 8 of this Agreement shall be responsible for informing the COT Agreement Manager of the termination of access.

17. SUBCONTRACTING

COT will not subcontract work or services contemplated under this Agreement and/or use an outside consultant except as provided for in the individual Statement of Work(s) without obtaining the prior written approval of ESD. COT acknowledges that such approval does not relieve its responsibility for Subcontractor compliance with all the terms and conditions of this Agreement.

18. NONDISCRIMINATION

No individual shall be excluded from participation in, denied the benefits of, subjected to discrimination under, or denied employment in the administration of or in connection with any provision of this Agreement because of race, color, creed, marital status, religion, sex, national origin, Vietnam-Era or disabled veteran’s status, age, the

presence of any sensory, mental or physical disability, or political affiliation or belief, provided that the prohibition against discrimination in employment because of disability shall not apply if the particular disability prevents the individual from performing the essential functions of his or her employment position, even with reasonable accommodation. The parties agree to abide by the standards of responsibility toward the disabled as specified by the Americans with Disabilities Act and applicable state law. In the event that one of the parties refuses to comply with the above provision, this Agreement may be canceled, terminated, or suspended in whole or in part by the other party.

19. RECORDS MAINTENANCE

Both parties shall retain all records, books or documents related to this Agreement for six (6) years beyond the expiration/termination of this Agreement. Federal auditors and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this period.

20. INDEMNIFICATION AND INSURANCE

20.1 To the fullest extent permitted by law, COT shall indemnify, defend, and hold harmless the state of Washington, ESD, and all officials, agents, and employees of State, from and against all claims for injuries or death to the extent arising out of or resulting from the City's negligent performance of this Agreement. COT's obligation to indemnify, defend, and hold harmless includes any claim by COT's agents, employees, representatives, or its employees.

COT expressly agrees to indemnify, defend, and hold harmless the State for any claim arising out of or incident to COT's or any Subcontractor's performance or failure to perform this Agreement. COT's obligation to indemnify, defend and hold harmless the State shall not be eliminated or reduced by any actual or alleged concurrent negligence of State or its agents, agencies, employees or officials.

COT waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend and hold harmless State and its agencies, officials, agents or employees.

20.2 COT shall provide insurance coverage, which shall be maintained in full force and effect during the term of this Agreement, as follows:

20.2.1 Commercial General Liability Insurance Policy. Provide a Commercial General Liability Insurance Policy, including contractual liability, in adequate quantity to protect against legal liability arising out of Agreement activity but no less than One Million dollars ($1,000,000) per occurrence. Additionally, the COT is responsible for ensuring that any Subcontractors provide adequate insurance coverage for the activities arising out of subcontracts.

20.2.2 Automobile Liability. In the event that services delivered pursuant to this Agreement involve the use of vehicles, either owned or unowned

by the COT, automobile liability insurance shall be required. The minimum limit for automobile liability is:

One million dollars per occurrence, using a Combined Single Limit for bodily injury and property damage.

20.2.3 Cyber Liability Coverage for Network Security and Privacy (cyber liability) insurance coverage of not less than one million dollars ($1,000,000) per occurrence or claims made for wrongful acts and four million dollars ($4,000,000) annual aggregate to be maintained for the duration of the agreement and one (1) year following its termination to respond to privacy and network security liability claims caused by COT.

20.2.4 The insurance required shall be issued by an insurance company/ies authorized to do business within the state of Washington, and shall name the state of Washington, its agents and employees as additional insureds under the insurance policy/policies. All policies shall be primary to any other valid and collectable insurance. COT shall instruct the insurers to give Agency thirty (30) days' advance notice of any insurance cancellation.

20.3 If self-insured, the COT warrants that it will maintain coverage sufficient to cover any liability specified above that may arise from the performance of this Agreement, and that the COT 's Risk Officer or appropriate individual will provide to the Agency evidence of such insurance.

20.4 The COT will provide the Agency with a copy of the applicable insurance facesheet(s) or certification of self-insurance reflecting these coverages and limits as defined in this section. Insurance coverage(s) must be effective no later than the effective date of this Agreement and for the term of this Agreement. COT shall submit renewal certificates as appropriate during the term of this Agreement.

21. DISPUTES

Except as otherwise provided in this Agreement, when a dispute arises between the parties and it cannot be resolved by direct negotiation, the parties agree to participate in non-binding mediation in good faith. The mediator shall be chosen by agreement of the parties. If the parties cannot agree on a mediator, the parties shall use a mediation service that selects the mediator for the parties. Nothing in this Agreement shall be construed to limit the parties' choice of a mutually acceptable alternative resolution method such as a dispute hearing, a Dispute Resolution Board, or arbitration.

22. NOTICE OF NONDISCLOSURE

COT agrees that all their authorized personnel who will have access to the information provided by ESD will sign a Notice of Nondisclosure, identical to that in Exhibit B, Notice of Nondisclosure. The statement is consistent with RCW 50.13 and the terms

and conditions of this Agreement. No data may be released to any COT personnel until ESD receives the completed Notice of Nondisclosure for that individual.

23. RIGHT OF INSPECTION

COT shall provide access to ESD, or any of its officers, or to any other authorized agent or official of the state of Washington or the federal government at all reasonable times, in order to monitor, evaluate and ensure the requirements of the state and federal statutes, related regulations, and this Agreement are being met. COT agrees to accommodate ESD's request for inspection, electronic monitoring, review, or audit and to allow on-site audits during regular business hours.

24. WAIVER

Any waiver by any party with regard to any of its rights shall be in writing and shall not constitute a waiver of any other or future rights of the party.

25. PENALTIES

COT understands and acknowledges that it has an affirmative obligation to take all reasonable actions necessary to prevent disclosure of Confidential UI Data. Any redisclosure of information under Section 11, must be expressly permitted by ESD and documented in an amendment to this Agreement prior to any re-disclosure. Failure to obtain ESD's prior approval could subject the recipient to fines pursuant to RCW 50.13.110.

As stated in Section 9.4, if misuse or unauthorized disclosure occurs, all parties aware of the violation must inform ESD immediately but in no event more than 24 hours. The COT must take all reasonable available actions to rectify the disclosure to ESD's standards.

26. SEVERABILITY

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, and to this end the provisions of this Agreement are declared to be severable.

27. TERMINATION

27.1 This Agreement shall remain in full force and effect until terminated as provided in this Agreement. Either party may terminate this Agreement by giving ten (10) calendar days' written notice to the other party. The obligations of confidentiality shall continue and survive this Agreement.

27.2 In the event of termination of this Agreement, COT shall be liable to ESD due for payment of services rendered by ESD that met the requirements of Exhibit A,

Statement of Work and shall return or destroy UI Data to ESD on or before the effective date of termination, according to section 9.1 of this Agreement.

27.3 Immediately following termination or expiration of this Agreement for any reason, COT shall cease any and all use and distribution of the UI Data, information and services derived therefrom, related documentation, and all other information and materials provided by ESD to COT under the Agreement, and COT shall at its sole cost return, delete, or destroy UI Data then in its possession or under its control pursuant to Section 9.1 of this Agreement including, without limitation, originals, and copies of such UI Data and provide certification thereof all of the foregoing items and materials to ESD within 60 days of such termination or expiration.

27.4 COT agrees to certify that UI Data has been returned, deleted, or destroyed from its systems, servers, off-site storage facilities, office locations, and any other location where COT maintains UI Data within 60 days of termination. COT shall document its verification of data removal, including tracking of all media requiring cleaning, purging or destruction.

The failure to follow this section may subject the COT to the penalties stated in Section 25.

28. TERMINATION FOR CAUSE

Either party may terminate this Agreement in whole or in part at any time prior to the date of completion when it is determined that the other party has failed to comply with the conditions of this Agreement. The terminating party shall immediately notify the other party in writing of the termination and the reasons for termination, together with the effective date of termination.

29. TERMINATION FOR FUNDING REASONS

In the event funding from state, federal, or other sources is withdrawn, reduced, or limited in any way after the effective date of this Agreement and prior to normal completion, the affected party may unilaterally terminate this Agreement. Written notification of termination shall be mailed return receipt requested. Such action is effective upon receipt of the written notification.

30. SUBPOENA

Should COT receive a subpoena for UI Data, COT must meet the requirements of 20 CFR 603.7, prior to producing the UI Data subject to the subpoena.

With respect to other information, should either party receive a request or subpoena that would, fairly construed, seek production of privileged information that it received pursuant to this Agreement, the party receiving such a request or subpoena shall take reasonable measures, including but not limited to asserting the common interest privilege, to preclude or restrict the production of such information for ten (10)

business days, and shall promptly notify the donor agency that such a request or subpoena has been received, so that the donor agency may file any appropriate objections or motions, or take any other appropriate steps, to preclude or condition the production of such information.

31. JURISDICTION

This Agreement shall be construed and interpreted in accordance with the laws of the State of Washington. The venue of any legal action pertaining to this Agreement shall be the Washington State Superior Court for Thurston County. All parties agree to the exclusive jurisdiction of such court and waive any right to challenge jurisdiction or venue.

32. AGREEMENT AMENDMENTS

This Agreement may be waived, changed, modified, or amended only by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

33. ASSURANCES

The parties agree that all activity pursuant to this Agreement will be in accordance with all applicable current or future federal, state, and local laws, rules, and regulations.

34. ASSIGNMENT

Neither party shall assign this Agreement in whole or in part.

35. DISCLAIMER

Exchange of UI Data pursuant to this Agreement is not a public disclosure under RCW 42.56.

36. ORDER OF PRECEDENCE

In the event of an inconsistency in this Agreement, unless otherwise provided, the inconsistency shall be resolved by giving precedence in the following order:

1. Applicable Federal and State Statutes and Regulations;
2. Applicable Statement(s) of Work;
3. Any other provisions of this Agreement, including the attached Exhibits.

37. SURVIVAL OF TERMS

The provisions of Section 9 “Data Disposal; Permissible Use; Breach”, Section 10 “Physical Safeguards & Security”, Section 11 “Redisclosure of Information”, Section 19 “Records Maintenance”, Section 25 “Penalties”, Section 27 “Termination” shall survive the termination of this Agreement for any reason.

38. ALL WRITINGS CONTAINED HEREIN

This Agreement sets forth in full the entire agreement of the parties; and any other agreement, representation, or understanding, verbal or otherwise, is hereby deemed null and void and of no force and effect whatsoever.

By signing this Agreement, both parties certify that their policies and procedures comply with the confidentiality requirements of this Agreement.

The parties hereby agree to execute this Agreement.

Washington State Employment Security Department	**City of Tacoma**
Emily Jitske Kok	Danielle Larson
By (print name)	By (print name)
Chief Data Privacy Officer	Tax & License Manager
Title	Title
Signature	Signature
Date	Date

EXHIBIT A

STATEMENT OF WORK # 1

1. PURPOSE

This Statement of Work establishes the terms and conditions under which ESD will share certain confidential UI Data with COT for the purpose of verifying and enforcing tax and license requirements of the Tacoma Municipal Code Title 6 – Tax & License Code.

2. PERMISSIBLE USE

Use of Confidential UI Data by COT under this Statement of Work is limited to the following objectives:

2.1 Verification of the number of employees qualifying an employer for City Business & Occupation Tax Credits.

2.2 Verification that an employer is engaged in business in Tacoma indicted by employees located in Tacoma.

2.3 Verification of Tacoma vs State-wide payroll figures to determine the payroll factor used in the City's two-factor Service & Other Apportionment calculation which consists of a gross receipts factor and a payroll factor.

2.4 Verification that employees are paid at least a "Family wage" or state minimum wage qualifying an employer for certain City Business & Occupation Tax Credits.

2.5 Presenting UI data that does not identify individuals or entities for the purpose of reviewing impacts from potential new policy decisions, such as new tax or license laws being reviewed for implementation in the Tacoma Municipal Code.

2.6 Verification that persons requiring a state or local regulatory license is an employee and not a contractor for hire at businesses operating in Tacoma.

3. DATA ELEMENTS TO BE DISCLOSED

ESD shall provide the following data elements to authorized COT employees for the purposes of carrying out activities described in this Statement of Work, Section 2. PERMISSIBLE USE.

Parameters for the data elements are as follows:

Area: Pierce County Employer Data.

Time Period: Current Quarter plus four years historical data.

ESD Data Source: QCEW (Quarterly Census of Employment & Wages) data.

- STATE_FIPS
- YearQuarter
- EAN (Employer Account Number)
- RUN (Reporting Unity Number to distinguish locations)
- LEGAL_NAME
- Trade_NameDBA
- PLA_LINE_1
- PLA_LINE_2
- PLA_ADD_CITY
- PLA_ADD_STATE
- PLA_ADD_ZIP
- PLA_ADD_ZIPEXT
- TacomaEmp --the total employed by employer in city of Tacoma
- TacomaWage --the total wages paid by employer in city of Tacoma
- MEEI_Code – Multiple Establishment Employer Indicator
- WaEmp – the total employed by the Tacoma [SN(1] employer in the state
- WaWage– the total wages paid by the Tacoma employer in the state

4. FREQUENCY OF DATA TRANSFER AND SECURITY

Initial transfer will include 4 years of historical data. Subsequent updates will be provided on a quarterly basis through MFT, with the occasional request in between for time sensitive data. .

UI Confidential Data must be provided to COT on a secured MFT (Managed File Transfer) server or similar approved by ESD.

Describe the specific secure medium used for data transfer: MFT

5. NOTICE OF NONDISCLOSURE

Authorized COT staff that review or work with UI Data must read and sign the ESD Notice of Nondisclosure prior to viewing or working with the data. Signed copies of Notice of Nondisclosure shall be returned to the ESD Data Sharing Office at DataSharingSupport@esd.wa.gov. The ESD Notice of Nondisclosure is incorporated by reference to this Agreement as Exhibit "B".

6. AUTHORIZATION ON PUBLICATION OF CONFIDENTIAL DATA

- COT shall inform ESD before publication of any report including UI Data and share any drafts of work products at least ten (10) working days prior to public release.
- Release of information derived from confidential ESD's data, other than to the authorized members or staff must be aggregated in such a manner that individual data cannot be identified in any grouping level.
- Groupings at any aggregate level must be in such a manner that when combined with other publicly available information would not reveal the name or any identifying particular about any individual or entity.

7. PERIOD OF PERFORMANCE

The Period of performance for this Statement of Work shall commence on the date of execution and shall continue through 31 July 2028 unless terminated sooner as provided in the Agreement.

8. STATEMENT OF WORK AMENDMENTS

This Statement of Work may be waived, changed, modified, or amended only by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

9. CONSIDERATION

If payment is required, ESD shall give COT advance notice of the expected charges and an opportunity to approve the charges or to withdraw the data request. Reimbursement shall be within thirty (30) calendar days of receipt of properly executed invoice vouchers. Vouchers shall include such information as is necessary to determine the exact nature of the charges.

10. STATEMENT OF WORK MANAGEMENT

The work described herein shall be performed under the coordination of the following Statement of Work Managers or their successors, who will provide the assistance and guidance necessary for the performance of this Statement of Work.

COT staff member responsible for the management of this Statement of Work is:	**ESD staff member responsible for the management of this Statement of Work is:**
Kris Oldenburg	Barb Arnott
Audit and Compliance Manager	Data and Product Support Manager

747 Market Street
Tacoma, WA 98402

Phone: 253-573-2442
Email address:
koldenburg@cityoftacoma.org

212 Maple Park Ave SE
Olympia, WA 98501

Phone: 509-656-6705
Email address:
barb.arnott@esd.wa.gov

11. APPROVAL

Now, therefore, in consideration of the mutual promises and undertakings contained herein and in the Interagency Agreement it supplements, the parties hereto consent to the provisions of Exhibit A, Statement of Work # 1.

Washington State Employment Security Department	**City of Tacoma**
Gustavo Aviles	Danielle Larson
By (print name)	By (print name)
Chief Analytics Officer	Tax & License Manager
Title	Title
Signature	Signature
Date	Date

ESD Agreement #_____
COT Agreement #_____

EXHIBIT B

WASHINGTON STATE EMPLOYMENT SECURITY DEPARTMENT
NOTICE OF NONDISCLOSURE

As a non-Employment Security Department (ESD) employee, you may be given access to records or information that is deemed private and confidential by statute.

You may not make any unauthorized disclosure of private or confidential information about employers, clients/claimants or employees to any person or entity. Confidential information includes but is not limited to employee's wages or hours, unemployment insurance benefit records, and North American Industry Classification System (NAICS) codes of individual employers.

The unauthorized disclosure or abuse of information deemed private and confidential may subject you to a civil penalty of up to Twenty Thousand dollars ($20,000) in 2018, and annually adjusted as allowed in statute, and other applicable sanctions under state and federal law.

I have read and understand the above Notice of Nondisclosure.

_____ _____
Printed Name Job Title or User ID

_____ _____
Signature Date

The above individual has been informed of the obligations of the above referenced agreement and Statement of Work including any limitations, use or publishing of Confidential Data.

_____ _____
Supervisor's Name Agency Name

_____ _____
Supervisor's Signature Date

An original of this notice or DocuSign copy must be returned to the Employment Security Department.