DATA-SHARING AGREEMENT

BETWEEN THE

STATE OF WASHINGTON

DEPARTMENT OF RETIREMENT SYSTEMS,

PUBLIC EMPLOYER,

AND

UHY LLP CERTIFIED ACCOUNTANTS

This Agreement is made and entered into by and between the **DEPARTMENT OF RETIREMENT SYSTEMS, PUBLIC EMPLOYER,** and **UHY LLP Certified Accountants** pursuant to the authority granted in Chapters 39.34 and 41.50 of the Revised Code of Washington, relevant federal statutes, and related regulations.

AGREEMENT ADMINISTRATORS:

Department of Retirement Systems	**PUBLIC EMPLOYER**	**UHY LLC Certified Public Accountants**
Sarah White	NAME	Jason Ostroski
Petitions Examiner & DSA Coordinator	TITLE	Principal
	PUBLIC EMPLOYER	8601 Robert Fulton Drive, Suite 210
PO Box 48380	Address	
Olympia, WA 98504-8380	Address	Columbia, MD 21046
360-664-7205	Phone	410-423-4839
sarah.white@drs.wa.gov	Email	jostroski@uhy-us.com

1. PURPOSE OF THE DATA-SHARING AGREEMENT

Under WAC 415-117-030, every employer participating in one or more of the retirement systems is required to cooperate fully in the administration and audit of the retirement systems. Every year, the Department of Retirement Systems (DRS) selects employers to participate in census data testing. The selected employers must cooperate with DRS which includes, but is not limited to, confirming data and records in a timely manner. RCW 39.34.240 requires public agencies to sign a written agreement that documents how category 3 or higher data will be shared and protected.

The purpose of this Agreement is to allow PUBLIC EMPLOYER (PUBLIC EMPLOYER) to provide employee data to DRS' contractor, UHY LLP Certified Accountants (UHY) in fulfillment of DRS Contract No. 22-19, Audit Services for Financial Reporting of Governmental Pension Plans. DRS contracted with UHY to audit retirement system membership data, otherwise known as "census data." This requires testing payroll information and detailed information for certain employees. UHY and its employees will only use PUBLIC EMPLOYER data for purposes related to DRS Contract No. 22-19.

2. DEFINITIONS

"Agreement" means this Data-Sharing Agreement, including all documents attached or incorporated by reference.

"Authorized user" means an individual or individuals with an authorized business need to access Confidential Information under this DSA.

"Confidential Information" means information that is exempt from disclosure to the public or other unauthorized person under Chapter 42.56 RCW or other federal or state laws. Confidential Information comprises both Category 3 and Category 4 data as described in Section 3, Data Classification, which includes but is not limited to Personally Identifiable Information (PII). For purposes of this DSA, Confidential Information means the same as "Data."

"Data" means the information that is disclosed or exchanged as described by this DSA. For purposes of this DSA, Data includes PII and Confidential Information.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode Data to protect its confidentiality. Data encryption can be required during Data transmission or Data storage depending on the level of protection required for this Data.

"Data Storage" refers to the state Data is in when at rest. Data shall be stored on secured environments.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the Data between systems, networks, and/or workstations.

"Disclosure" means to permit access to or release, transfer, or other communication of PII by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record.

"Employee" means anyone on the payroll receiving compensation from PUBLIC EMPLOYER, regardless of retirement system membership. This includes but is not limited to employees who are members of a DRS covered retirement system, employees who are not members of a DRS covered retirement system, independent contractors, retirees who have returned to work, paid volunteers, elected officials, board members, and paid interns.

"Personally Identifiable Information" or "PII" means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Personally Identifiable Information also includes other information that, alone or in combination, would allow a reasonable person to identify the individual with reasonable certainty. In the case of employment Data, this means information 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 other publicly available information to reveal any such particulars.

"Security Incident" means the attempted or successful unauthorized access, use, Disclosure, modification or destruction of Data, information, or interference with system operations in an information system.

3. PERIOD OF AGREEMENT

This Agreement shall begin on the date of execution and end on December 31, 2025, unless extended in accordance with Section 12, or terminated sooner in accordance with Section 14.

4. DESCRIPTION OF DATA TO BE SHARED

The Data to be shared is classified as Category 3 (confidential) under Washington State Office of Cybersecurity *Data Classification Standard, SEC 08-01-S* as amended or superseded.

a. PUBLIC EMPLOYER will provide the following data to UHY:

i. A complete detailed payroll file that includes cumulative payroll data for all pay periods that fell between July 1, 2023 and June 30, 2024. Payroll data must be based on pay period ending dates, therefore payroll period dates may vary. It is important that the file include all employees and not just employees participating in a DRS plan. The file is to include the following data fields:

1. All employees paid (even non-participants)
2. Full Social Security Number
3. First and last name
4. Date of birth
5. Date of hire
6. Itemized gross wages (regular pay, sick pay, hazard pay, etc.)

Submitting the following additional data fields may reduce follow-up requests for information from UHY:

7. Itemized detail of hours (regular pay, sick pay, hazard pay, etc.)
8. Job title
9. Date of termination (if applicable)

ii. Copies of Form 941 filings as of September 30, 2023, December 31, 2023, March 31, 2024 and June 30, 2024.

1. UHY is aware the gross wages from the detailed payroll file will not tie to the federal wages in the Form 941 filings. However, the gross wages per the detailed payroll file will be compared to the Form 941 filings for reasonableness.

iii. Provide a breakdown of (1) payroll codes and whether they are considered reportable to DRS or not, as well as (2) job descriptions that are reportable or not. If this information cannot be queried in PUBLIC EMPLOYER's detailed payroll file, PUBLIC EMPLOYER may wait to provide it during the next phase of DRS' testing.

If any of the payroll fields do not apply or are not available within one comprehensive report, PUBLIC EMPLOYER will provide equivalent information as available.

iv. Information for a sample of approximately 25 employees, as identified by UHY following receipt and review of items (i), (ii), and (iii) listed above. The information may include but is not limited to: requests for eligibility documentation, additional detail and years of payroll data, documentation of employee hire and/or termination, contract information, and identification of employees who participate in another retirement system. Additional employee selections may be necessary in certain circumstances (i.e., identification of pervasive errors in sample) but UHY will work to limit such requests in an effort to minimize follow up items.

PUBLIC EMPLOYER and UHY may request additional information or clarification from each other as needed.

Data will be provided in an electronic format: Excel and CSV files are preferred; Word, PDF, or text files can be accepted if necessary; all other formats require approval.

UHY contact for questions about the secure file transfer process or required data:

Steve Maranto, SMaranto@uhy-us.com

b. UHY may provide DRS with data received under subsection (4)(a) of this Agreement, as needed, so that DRS may provide training or address questions or data discrepancies with PUBLIC EMPLOYER.

5. DATA TRANSMISSION

To ensure Data is encrypted during Data Transmission, all Data will be transmitted using a managed file transfer (MFT) platform that is security compliant with Washington State Office of Cybersecurity data encryption standards, *Encryption Standard, SEC 08-02-S* as amended or superseded. UHY will provide PUBLIC EMPLOYER with access to its MFT platform to facilitate the Data transfer. PUBLIC EMPLOYER will provide the Data outlined in subsection (4)(a) of this Agreement within fifteen (15) business days of either DRS' or UHY's request, unless otherwise agreed to.

6. DATA SECURITY

a. **Safeguards Against Unauthorized Access and Redisclosure.** UHY must protect and maintain all Data against unauthorized use, access, disclosure, modification, or loss. This requires UHY to employ reasonable security measures, which include restricting access to the Data by:

i. Allowing access only to staff, officials, and agents of UHY that have an authorized business requirement to view the Data who need it to perform their official duties in the performance of the work requiring access to the information as detailed in the Purpose of this Agreement. UHY will protect the Data to prevent unauthorized persons from retrieving information by means of a computer, remote terminal, or

other access. UHY will protect the Data to prevent unauthorized persons from retrieving information by means of a computer, remote terminal, online access, or other access.

ii. Physically securing any computers, documents, or other media that could be used to access the Data.

iii. All access to Data accessed or acquired by UHY under the terms of this Agreement, if retained in any manner or format, shall be stored and managed within a secure environment with access limited to the least number of employees needed to complete the purpose of this Agreement.

b. All parties will meet the requirements of the State of Washington Office of Cybersecurity's policies and standards for data security and access controls to ensure the confidentiality, availability, and integrity of all data accessed.

c. **Protection of Data** – UHY agrees to store Data and protect Data as described:

i. *Workstation storage drives*. Access to the Data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password in addition to Multifactor Authentication (MFA) which provide greater security, such as biometrics, authentication token devices, or smart cards. If the workstation is located in an unsecured physical location, the hard drive must be encrypted using the latest FIPS 140-2 approved encryption algorithm with a minimum key length of 256 bits to protect Data in the event the device is stolen.

ii. UHY employees may not store any Data on portable electronic devices or media, including but not limited to: laptops, handheld/PDAs, ultra-mobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), portable hard disks and smart phones at any time.

iii. UHY will store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

iv. UHY will protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

v. UHY shall instruct all individuals with access to the Personally Identifiable Information regarding the confidential nature of the information, the requirements of *Use of Data* and *Safeguards Against Unauthorized Access and Re-Disclosure* clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Agreement.

d. **Data Separation**

i. DRS data and PUBLIC EMPLOYER data must be separated or otherwise distinguishable from non-PUBLIC EMPLOYER and non-DRS data. This is to ensure

that when no longer needed by UHY, all DRS data and PUBLIC EMPLOYER data can be identified for return or destruction. It also aids in determining whether DRS data or PUBLIC EMPLOYER data has or may have been compromised in the event of a security breach.

ii. DRS data and PUBLIC EMPLOYER data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DRS data and non-PUBLIC EMPLOYER data. Or,

iii. DRS data and PUBLIC EMPLOYER data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DRS data and PUBLIC EMPLOYER data. Or,

iv. DRS data and PUBLIC EMPLOYER data will be stored in a database which will contain no non-DRS data and non-PUBLIC EMPLOYER data. Or,

v. DRS data and PUBLIC EMPLOYER data will be stored within a database and will be distinguishable from non-DRS data and non-PUBLIC EMPLOYER data by the value of a specific field or fields within database records. Or,

vi. When stored as physical paper documents, DRS data and PUBLIC EMPLOYER data will be physically separated from non-DRS data and non-PUBLIC EMPLOYER data in a drawer, folder, or other container that is secured against unauthorized access.

vii. When it is not feasible or practical to separate DRS data and PUBLIC EMPLOYER data from non-DRS data and non-PUBLIC EMPLOYER data, then both the DRS data and PUBLIC EMPLOYER data the non-DRS data and non-PUBLIC EMPLOYER data with which it is commingled must be protected as described in this Agreement.

If UHY or its agents detect a compromise or potential compromise in the IT security for this data such that Confidential Information may have been accessed or disclosed without proper authorization, UHY shall give notice to DRS and PUBLIC EMPLOYER within twenty-four (24) hours of discovering the compromise or potential compromise. Notice to DRS can be by phone with follow-up email if unable to speak to a live person. Contacts for purposes of this section are:

Chief Information Security Officer
Gary Nicholas, (360) 664-7057, gary.nicholas@drs.wa.gov

Information Services Division Assistant Director
Jay Walsh, (360) 664-7266 or (m) (360) 701-3723, jay.walsh@drs.wa.gov

Please cc: **Risk Management Director**
Julie Amos, (360) 664-7983, julie.amos@drs.wa.gov

UHY shall take corrective action as soon as practicable to eliminate the cause of the breach and shall be responsible for managing the incident response, as required by law or regulation, including reporting the incident to WATech and ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed. DRS

may, at its discretion, assist with the response. UHY is responsible for any costs associated with the incident, regardless of whether it is a DRS, PUBLIC EMPLOYER, or UHY cost, excluding staff assistance. DRS, PUBLIC EMPLOYER, and UHY must remain in full communication and coordination throughout the planning and implementation of the incident response.

7. DATA CONFIDENTIALITY

UHY acknowledges the personal or confidential nature of the information and agrees that their employees and subcontractors with access shall comply with all laws, regulations, and policies that apply to protection of the confidentiality of the Data.

UHY will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained under this DSA for any purpose that is not directly connected with the purpose, justification, and Permissible Uses of this DSA, and of DRS Contract No. 22-19, except as provided by law.

a. **Subcontractors**

Data access shall not be provided to any subcontractor under this Agreement.

b. **Penalties for Unauthorized Disclosure of Information**

In the event that either party fails to comply with any terms of this Agreement, the other party shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

8. USE OF DATA

The Data being shared is owned by DRS and PUBLIC EMPLOYER. This Agreement does not constitute a release of the Data for UHY's discretionary use. UHY must use the Data received or accessed under DRS Contract No. 22-19 or this Agreement only to carry out the purposes and justifications of the Contract and Agreement. Any analysis, use, or reporting that is not within the purposes of the Contract and Agreement are not permitted.

Any disclosure of Data contract to this Agreement is unauthorized and is subject to penalties identified by law and the obligations under DRS Contract No. 22-19.

9. DISPOSITION OF DATA

Upon termination of this Agreement, all copies of any Data sets related to this Agreement must be destroyed, wiped from data storage systems, or must be returned to DRS or PUBLIC EMPLOYER. As outlined in DRS Contract No. 22-19 Exhibit D-Attachment A, UHY must document its disposal of Data and timely notify DRS.

Acceptable destruction methods for various types of media include:

a. For paper documents/reports containing confidential or sensitive information, a contract with a recycling firm to recycle confidential documents is acceptable, provided the contract

ensures that the confidentiality of the Data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

b. For paper documents containing confidential information requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.

c. Data will be disposed of by deletion when stored on a portal, server or workstation, in accordance with Washington State Office of Cybersecurity, *Media Sanitization and Disposal Standard,* SEC-04-02-S, a National Institute for Standards and Technology (NIST) compliant sanitation wipe process will be performed upon end of life, or event that requires the media to leave UHY organizational control. The sanitation process will consist of no less than three (3) overwriting passes using a fixed or random data value or using the Cryptographic Erase (CE) technique, ensuring data cannot be reconstructed. Failed drive(s) unable to follow the aforementioned sanitation process will be physically destroyed by a certified vendor.

10. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

This Agreement will take place remotely, however, if on DRS or PUBLIC EMPLOYER premises, UHY, its agents or employees will comply, in all respects, with DRS or PUBLIC EMPLOYER physical, fire, access, safety, and security requirements.

UHY will maintain records as described in DRS Contract No. 22-19: UHY shall maintain books, records, documents, and other evidence pertaining to DRS Contract No. 22-19 to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. UHY shall retain such records for a period of six (6) years following expiration or termination of DRS Contract No. 22-19 or final payment, whichever is later; Provided, however, that if any litigation, claim, or audit is commenced prior to the expiration of this period, such period shall extend until all such litigation, claims, or audits have been resolved.

11. HOLD HARMLESS

Each party to this Agreement shall be responsible for any and all acts and omissions of its own staff, employees, officers, agents and independent contractors. Each party shall defend and hold harmless the other party from any and all claims, damages, and liability of any kind arising from any act or omission of its own staff, employees, officers, agents, and independent contractors.

12. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT

With mutual consent, DRS, PUBLIC EMPLOYER, or UHY may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized representatives of both parties.

13. ORDER OF PRECEDENCE

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

a. Applicable Federal and State laws;

b. Any other provisions of the Agreement whether by reference or otherwise.

14. TERMINATION

a. For Convenience

Any party may terminate this Agreement with thirty calendar days' written notice to the other party's Agreement Administrator named on Page 1. In case of termination, any and all information provided by DRS pursuant to this agreement shall either be immediately returned to the DRS or immediately destroyed.

b. For Cause

Any party may terminate this Agreement at any time prior to the date of completion if and when it determines that the other party has failed to comply with the conditions of this Agreement. The terminating party shall promptly notify the other party in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the Data provided by one party shall be returned to the other party or destroyed on or before the date of termination. Written notification of destruction to the other party is required.

15. GOVERNING LAW

This Agreement shall be construed under the laws of the State of Washington. Venue shall be proper in Superior Court in Thurston County, Washington.

16. SEVERABILITY

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court; that invalidity shall not affect the other provisions of this Agreement and the invalid provision shall be considered modified to conform to the existing law.

17. SIGNATURES

The signatures below indicate agreement between the parties.

Department of Retirement Systems	**PUBLIC EMPLOYER**	**UHY LLC Certified Public Accountants**

Mike Ricchio Assistant Director Administrative Services Division	Name Title	Jason Ostroski Principal