INTERAGENCY DATA SHARING AGREEMENT

Between

City of Winlock

And the Office of the Washington State Auditor

This Interagency Data Sharing Agreement (DSA) is entered into by and between City of Winlock, hereinafter referred to as "Agency", and the Office of the Washington State Auditor, hereinafter referred to as "SAO", pursuant to the authority granted by Chapter 39.34 RCW, 42.40 RCW, 43.101 RCW and 43.09 RCW.

Agency:

Agency Name:	City of Winlock
Contact Name:	Penny Jo Haney
Title:	Clerk
Address:	323 NE First Street Winlock, WA 98596
Phone:	(360) 785-3811
E-mail:	cityclerk@cityofwinlock.com

SAO

Agency Name:	Office of the Washington State Auditor
Contact Name:	Lisa Carrell
Title:	Program Manager
Address:	3200 Sunset Way SE, Olympia, WA 98504
Phone:	(564) 999-0880
E-mail:	carrelll@sao.wa.gov

The SAO and Agency agree that they will have the right, at any time with reasonable notice, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance.

1. PURPOSE OF THE DSA
   The purpose of the DSA is to provide the requirements and authorization for the Agency to exchange confidential information with SAO and SAO to share confidential information with the Agency. This agreement is entered into between Agency and SAO to ensure compliance with legal requirements and Executive Directives (Executive Order 16-01, RCW 42.56, and OCIO policy 141, OCIO standard 141.10) in the handling of information considered confidential.

2. DEFINITIONS

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

"Data Access" refers to rights granted to SAO employees to directly connect to Agency systems, networks and/ or applications combined with required information needed to implement these rights.

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

"Data Storage" refers to the place data is in when at rest. Data can be stored on removable or portable media devices such as a USB drive or SAO managed systems or OCIO/ State approved services.

"Data Encryption" refers to enciphering data with a NIST-approved algorithm or cryptographic module using a NIST-approved key length. Encryption must be applied in such a way that it renders data unusable to anyone but the authorized users.

"Personal Information" means information defined in RCW 42.56.590(10).

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer. The Data that is the subject of this DSA is classified as indicated below:

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.

Category 2 – Sensitive Information Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to: a. Personal Information about individuals, regardless of how that information is obtained; b. Information concerning employee personnel records; c. Information regarding IT infrastructure and security of computer and telecommunications systems; d. List of individuals for commercial purposes.

Category 4 – Confidential Information Requiring Special Handling Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which: a. Especially strict handling requirements are dictated, such as by statutes, regulations, agreements, or other compliance mandates; b. Serious

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

3. PERIOD OF AGREEMENT
This agreement shall begin on June 1, 2024, or date of execution, whichever is later, and end on May 31, 2027, unless terminated sooner or extended as provided herein.

4. JUSTIFICATION FOR DATA SHARING
SAO is the auditor of all public accounts in Washington State. SAO's authority is broad and includes both explicit and implicit powers to review records, including confidential records, during the course of an audit or investigation.

5. DESCRIPTION OF DATA TO BE SHARED
The data to be shared includes information and data related to audit results, financial activity, operation and compliance with contractual, state and federal programs, security of computer systems, performance and accountability for agency programs as applicable to the audit(s) performed. Specific data requests will be limited to information needed for SAO audits, investigations and related statutory authorities as identified through auditor requests.

6. DATA TRANSMISSION
Transmission of data between Agency and SAO will use a secure method that is commensurate to the sensitivity of the data being transmitted.

7. DATA STORAGE AND HANDLING REQUIREMENTS
Agency and SAO will notify each other if they are providing confidential data. All confidential data provided by Agency will be stored using data encryption with access limited to the least number of SAO staff needed to complete the purpose of the DSA.

8. INTENDED USE OF DATA
The Office of the Washington State Auditor will utilize this data in support of their audits, investigations, and related statutory responsibilities as described in RCW 43.09 and 42.40.

9. CONSTRAINTS ON USE OF DATA
The Office of the Washington State Auditor agrees to strictly limit use of information obtained under this Agreement to the purpose of carrying out our audits, investigations and related statutory responsibilities as described in RCW 43.09 and 42.40.

10. SECURITY OF DATA
SAO shall take due care and take reasonable precautions to protect Agency's data from unauthorized physical and electronic access. SAO complies with the requirements of the OCIO 141.10 policies and standards for data security and access controls to ensure the confidentiality, and integrity of all data shared.

11. NON-DISCLOSURE OF DATA
SAO staff shall not disclose, in whole or in part, the confidential data provided by Agency to any individual or agency, unless this Agreement specifically authorizes the disclosure. Confidential data may be disclosed only to persons and entities that have the need to use the data to achieve

the stated purposes of this Agreement. In the event of a public disclosure request for the Agency's Confidential data, SAO will notify the Agency

a. SAO shall not access or use the data for any commercial or personal purpose.
b. Any exceptions to these limitations must be approved in writing by Agency.
c. The SAO shall ensure that all staff with access to the data described in this Agreement are aware of the use and disclosure requirements of this Agreement and will advise new staff of the provisions of this Agreement.

Agency staff shall not disclose, in whole or in part, the confidential data provided by SAO to any individual or agency, unless this Agreement specifically authorizes the disclosure. Confidential data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement. In the event of a public disclosure request for the SAO's data, Agency will notify the SAO

a. Agency shall not access or use the data for any commercial or personal purpose.
b. Any exceptions to these limitations must be approved in writing by SAO.
c. The Agency shall ensure that all staff with access to the data described in this Agreement are aware of the use and disclosure requirements of this Agreement and will advise new staff of the provisions of this Agreement.

12. DATA DISPOSAL

Upon request by the SAO or Agency, or at the end of the DSA term, or when no longer needed, Confidential Information/Data must be returned or destroyed, except as required to be maintained for compliance or accounting purposes.

13. INCIDENT NOTIFICATION AND RESPONSE

The compromise of Confidential Information or reasonable belief that confidential information has been acquired and/or accessed by an unauthorized person that may be a breach that requires timely notice to affected individuals under RCW 42.56.590 or any other applicable breach notification law or rule must be reported to the Agency contact.

If the Receiving Party does not have full details about the incident, it will report what information it has and provide full details within 15 business days of discovery. To the extent possible, these initial reports must include at least: A. The nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery; B. A description of the types of information involved; C. The investigative and remedial actions the Receiving Party or its Subcontractor took or will take to prevent and mitigate harmful effects and protect against recurrence; D. Any details necessary for a determination of whether the incident is a breach that requires notification under RCW 42.56.590, or any other applicable breach notification law or rule. E. Any other information SAO or Agency reasonably requests.

14. OVERSIGHT

The SAO and Agency agree that they will have the right, at any time with reasonable notice, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance.

15. TERMINATION

Either party may terminate this Agreement with 30 days written notice to the other party's Agency Contact named on Page 1. However, once data is accessed by the SAO or Agency, this Agreement is binding as to the confidentiality, use of the data, and disposition of all data received as a result of access, unless otherwise amended by the mutual agreement of both parties.

16. AWARENESS AND TRAINING

SAO and the agency shall ensure that all staff with access to the data shared through this Agreement are aware of the use and disclosure requirements of OCIO 141.10 and RCW 42.56.590. SAO will comply with all state requirements and training regarding handling, storage and transmission of confidential data.

17. DISPUTE RESOLUTION

In the event that a dispute arises under this Agreement, a Dispute Board shall determine resolution in the following manner. Each party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review facts, contract terms, and applicable statutes and rules and make a determination of the dispute.

18. GOVERNANCE

a. The provisions of this Interagency Data Sharing 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 Interagency Data Sharing Agreement and the invalid provision shall be considered modified to conform to the existing law.
b. In the event of a lawsuit involving this Interagency Data Sharing Agreement, venue shall be proper only in Thurston County, Washington.

19. SIGNATURES

The signatures below indicate agreement between the parties.

Agency	Office of the Washington State Auditor
1/23/24	Lisa Carrell 1/22/24
Signature Date	Signature Date
Title: Mayor	Title: Program Manager