**INTERAGENCY DATA SHARING AGREEMENT**

**between the**

**STATE OF WASHINGTON**

**­­­­­­­­­­­­­­­Department of\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**and the**

**<AGENCY>**

This Interagency Data Sharing Agreement (DSA) is entered into by and between \_\_\_\_\_\_\_\_\_\_\_\_\_\_, hereinafter referred to as “\_\_\_\_”, and the <Agency>, hereinafter referred to as “<AGENCY>”, pursuant to the authority granted by Chapter 39.34 RCW.

***AGENCY PROVIDING DATA: <AGENCY>***

|  |  |  |
| --- | --- | --- |
| Agency Name |  |  |
| Contact Name(s): | Agreement Administrator: | Technical Administrator: |
| Title: |  |  |
| Division: |  |  |
| Address: |  |  |
| Phone: |  |  |
| E-mail: |  |  |

***AGENCY RECEIVING DATA: (Referenced in this document as Receiving Party (XXX) for example purposes only. The correct name or initials of the agency, and whichever role is appropriate for <AGENCY>, will be used in the final document.)***

|  |  |  |
| --- | --- | --- |
| Agency Name |  |  |
| Contact Name(s): | Agreement Administrator: | Technical Administrator: |
| Title: |  |  |
| Division: |  |  |
| Address: |  |  |
| Phone: |  |  |
| E-mail: |  |  |

This DSA has been reviewed by the authorized IT Data Security Administrator in each agency, as applicable.

1. **PURPOSE OF THE DSA**

The purpose of this DSA is to provide the XXX . . .

1. **DEFINITIONS**

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

“Data Access” refers to rights granted to XXX employees to directly connect to <AGENCY> systems, networks and /or applications via the State Governmental Network (SGN) 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 APD systems and XXX systems, networks and/or employee workstations.

“Data Storage” refers to the state data is in when at rest. Data can be stored on off-line devices such as CD’s or on-line on XXX servers or XXX employee workstations.

“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.

“Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver’s license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

1. **PERIOD OF AGREEMENT**

**This Agreement shall begin on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, or date of execution, whichever is later, and end on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, unless terminated sooner or extended as provided herein.**

1. **AUTHORITY and REASON FOR DATA SHARING**

The legal authority for sharing data identified in this agreement is …

Data is needed to . . .

1. **DESCRIPTION OF DATA TO BE SHARED**

*(****NOTE:*** *Include a description of the data that is requested, including classification/category of data, data elements, time frames for data disclosure or exchange (both when and for how long) and format of the data, as necessary. Specify if the data provided can be linked to other data and under what conditions, as necessary. For example: Data shared will include the data contained in the agency’s internal database that is described in this Agreement and will be updated through an automated process that runs daily on a server operated at . . . .).*

Data to be shared includes . . . .

1. **DATA ACCESS**

***Example:*** *Access methods for the shared data - Data access will be via terminal emulation software to be loaded on the appropriate XXX staff workstations. <AGENCY> will grant access permissions required to access the data defined above. Requirements for Access - Access to Data shall be limited to staff whose duties specifically require access to such Data in the performance of their assigned duties.*

**7. DATA TRANSMISSION**

*Example: Data transmission will be via anonymous FTP using the State Governmental Network (SGN) – The FTP site will be server ABC123, e-mail attachment, sneaker net, floppy disk, CD, etc. (pick one).*

**8. DATA STORAGE, DISPOSAL, AND HANDLING REQUIREMENTS**

***NOTE****: <AGENCY> needs to identify and include any constraints on XXX’s handling of the data once in XXX’s possession and proper disposal when no longer needed. Below paragraph is an example only.*

***Example:*** *All data provided by <AGENCY> will be stored in an encrypted form on a server with access limited to the least number of XXX staff needed to complete the purpose of this DSA. Data Disposal. At the end of the contract or when the data is no longer needed, data shall be returned to <AGENCY> or destroyed via an authorized method. Acceptable methods of destruction are as follows…*

*Example: Data stored for backup purposes. Data may be stored on portable media or non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of XXX’s existing, documented backup process for business continuity or disaster recovery purposes. Data must be protected and disposed of as required by this agreement.*

**9. DATA ENCRYPTION *(If applicable)***

***Example:*** *<AGENCY> and XXX have agreed to use a software tool to encrypt data prior to transmission and during Data Storage. The tool is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Example: PKZIP PRO; the encryption algorithm to be use is Password + 3DES). The password will be transmitted separately from any data transmission event.*

**10. INTENDED USE OF DATA**

***Example****: The data described above shall be used for analysis purposes only to prepare required annual business summaries published by XXX. Specify operations permitted.*

**11. CONSTRAINTS ON USE OF DATA**

This Agreement does not constitute a release of the data for the *XXX*’s discretionary use, but may be accessed only to carry out the responsibilities specified in RCW . . . . and for the purposes described herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of <AGENCY>.

*If Applicable* - The raw data and analysis generated will not identify personal information by name, and will be used for summary reporting purposes only. Any and all reports utilizing the data shall be subject to review by \_\_\_\_\_ prior to publication or presentation.

The *XXX* is not authorized to update or change any data in the \_\_\_\_\_\_\_ system, and any updates or changes will be cause for immediate termination of this Agreement.

**12. SECURITY OF DATA**

**A. Data Protection**

XXX shall take due care and take reasonable precautions to protect <AGENCY>’s data from unauthorized physical and electronic access. XXX will strive to meet or exceed the requirements of the Information Services Board (ISB) policies and standards for data security and access controls to ensure the confidentiality, availability and integrity of all data shared.

**B. Data Security Technology Standards**

<AGENCY> will be responsible for providing data security technology standards that will ensure acceptable levels of data security to XXX. These data security technology standards will include clear definitions outlining when and where data should be encrypted and by what technologies.

***Example:*** *<AGENCY> requires XXX to use the DIS Secure FTP service. <AGENCY> will cover all costs associated with this service.*

**C. IT Data Security Administration**

<AGENCY> and XXX IT Data Security Administrators will exchange documentation that outlines the data security program components supporting this Agreement. This documentation will define all data security methods and technology for each individual data exchange to ensure <AGENCY> and XXX are in compliance with all appropriate ISB security standards.

This documentation will serve to satisfy any potential requirement each agency may have under ISB Security Standards to document the management of secure information.

**13. NON-DISCLOSURE OF DATA**

Before receiving the data identified above, the XXX shall notify all staff who will have access to the data of the following requirements. This notification shall include all IT support staff as well as staff who will use the data. A copy of this notification shall be provided to <AGENCY> at the same time it is provided to relevant XXX staff.

1. **Non-Disclosure of Data**
2. XXX staff shall not disclose, in whole or in part, the data provided by <AGENCY> to any individual or agency, unless this Agreement specifically authorizes the disclosure. 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.
3. XXX shall not access or use the data for any commercial or personal purpose.
4. Any exceptions to these limitations must be approved in writing by <AGENCY>.
5. **Penalties for Unauthorized Disclosure of Information**

In the event the XXX fails to comply with any terms of this Agreement, <AGENCY> 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.

The XXX accepts full responsibility and liability for any violations of the Agreement.

1. **Employee Awareness of Use/Non-Disclosure Requirements**

The XXX 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.

XXX will provide an annual reminder to staff of these requirements. ***(Optional)***

**14. DATA CONFIDENTIALITY**

**(*NOTE****: Include these terms if the data is confidential. If the data being accessed by the XXX includes Protected Health Information, as defined in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, include Business Associate required terms as applicable. See* [*https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html*](https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html)*)*

* 1. Regulations Governing Confidentiality of Data

1. The *XXX* acknowledges the confidential nature of the information and agrees that *XXX* personnel with access shall comply with all laws, regulations and policies that apply to protection of the confidentiality of the data.
2. This data is confidential under state (NOTE: include if applicable: and Federal law), access and use of this information will be limited only to persons whose staff function requires such access.
   1. Limited Access to Data (Use as Applicable)

Individuals will access data only for the purpose of this Agreement. Each individual with data access shall read and sign Exhibit A, “Statement of Confidentiality and Non-Disclosure,” prior to access to the data.

**15. OVERSIGHT**

The XXX agrees that <AGENCY> will have the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance therewith, within the limits of RP’s technical capabilities.

**16. INCIDENT RESPONSE**

The XXX will provide prompt notice to <AGENCY> of any incident that may be a breach that requires notice to affected individuals under RCW 42.56.590, RCW 19.255.010, or any other applicable breach notification law or rule.

***NOTE***: Include additional details about how quickly after discovery notice must be provided, where notice is sent, who is responsible for determining whether the incident is a breach, who is responsible for sending notice to individuals and who is responsible for costs associated with the incident response.

**17. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT**

With mutual consent, <AGENCY> and the XXX may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff.

**18. TERMINATION**

Either party may terminate this Agreement with *(15, 20, 30)* days’ written notice to the other party’s Agreement Administrator named on Page 1. However, once data is accessed by the XXX, 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.

**19. 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 the facts, contract terms, and applicable statutes and rules and make a determination of the dispute.

**20. GOVERNANCE**

1. 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.
2. In the event of a lawsuit involving this Interagency Data Sharing Agreement, venue shall be proper only in Thurston County, Washington.

**21. SIGNATURES**

The signatures below indicate agreement between the parties.

**<AGENCY> DEPARTMENT OF\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date Signature Date

###### 

*TITLE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ TITLE: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*