# Data Share Agreement Sample

Overarching agreement for multi-party relationship

Entering data sharing agreements (DSAs) is a legal requirement and best practice when a third party receives or has access to Category 3 or 4 information. The terms of the agreement, however, may vary significantly depending on context, including the type of information, type of sharing, and the parties involved. Agencies may be flexible in determining appropriate DSA language but should also exercise sound discretion to ensure relationships are accurately documented and information is appropriately protected.

This sample can be used as one example of a DSA tailored for use when there are several parties involved, and the nature of the sharing makes it infeasible to document each data transmission with specificity in the contract.

The portions of the sample that are highlighted and/or in brackets require additional tailoring for use in a specific scenario by a specific agency. Beyond that, the terms overall should be reviewed to ensure they accurately describe the information, constraints and applicable security requirements. This sample does not necessarily include all terms that should be included in all scenarios. Agencies may review the Office of Privacy and Data Protection’s Data Sharing Agreement Implementation Guidance for additional support.

While this sample and the Data Sharing Agreement Implementation Guidance are intended to be resources that can help agencies assess options, they are not provided for the purpose of giving legal advice of any kind. This sample does not represent the legal opinion of any Washington state agency. Readers should not rely on information in this guide regarding specific applications of the laws without seeking legal counsel.

### Background

[If helpful, include background that would provide additional context for the data sharing relationship beyond what is included in section 2.]

### Purpose and Authority for Data Sharing

The Confidential Information to be shared under this DSA is shared . . . [Explain the purpose and authority for sharing. If the information is shared to help fulfill statutorily authorized functions, cite to those statutes. If the sharing is specifically allowed or required by statute, rule or other authority, cite to that authority.]

The purpose of this DSA is to identify, describe and protect the Confidential Information that will be shared between the Parties.

### Definitions

**[“Agency”]** means \_\_\_\_\_\_, any section, unit or other entity at [Agency], or any of the officers or other officials lawfully representing [Agency]. [Provide separate definition for each Party.]

**“Agreement”** means this Data Share Agreement.

**“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 persons 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 6, *Data Classification*, which includes, but is not limited to, Personal Information. For purposes of this DSA, Confidential Information means the same as “Data.”

**“Contract Administrator”** means the individual designated to receive legal notices and to administer, amend, or terminate this DSA.

**“Contract Manager”** means the individual identified on the cover page of this DSA who will provide oversight of the activities conducted under this DSA.

**“Data”** means the information that is disclosed or exchanged as described by this DSA. For purposes of this DSA, Data means the same as “Confidential Information.”

**“Disclosing Party”** means any party disclosing Confidential Information pursuant to this DSA, and includes the entity’s owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

**“Disclosure”** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

**“DSA”** means this Data Share Agreement.

**“RCW”** means the Revised Code of Washington. All references in this DSA to RCW chapters or sections will include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at: <http://apps.leg.wa.gov/rcw/>.

**“Regulation”** means any federal, state, or local regulation, rule, or ordinance.

**“Receiving Party”** means any party receiving Confidential Information pursuant to this DSA, and includes the entity’s owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

**“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

**“Subcontract”** means any separate agreement or contract between a Receiving Party and an individual or entity (“Subcontractor”) to perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

**“Subcontractor”** means a person or entity that is not in the employment of the Receiving Party, who is performing services or any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

**“WAC”** means the Washington Administrative Code. All references in this DSA to WAC chapters or sections will include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at: <http://apps.leg.wa.gov/wac/>.

### Description of Data to be Shared

* 1. The Data that will be shared includes: [Describe the confidential information that will be shared with as much specificity as possible.]
	2. The Data will be shared:

[Describe when the information will be shared, such as at specific intervals, as needed or at the request of a Receiving Party.]

[Describe how the information will be transferred, such as via secure file transfer or secure email.]

* 1. The Disclosing Party shall identify the Data it considers Category 3 pursuant to OCIO Standard No. 141.10 and chapter 42.56 RCW.

### Data Classification

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 (OCIO) and included in OCIO Standard No. 141.10.

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 release or disclosure by law. It may include but is not limited to:

1. Personal Information about individuals, regardless of how that information is obtained;
2. Information concerning employee personnel records;
3. Information regarding IT infrastructure and security of computer and telecommunications systems;

[ ]  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:

1. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
2. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

### Constraints on Use of Data

* 1. The Data being shared is owned by the Disclosing Party that created it. In some cases, the Data may represent Confidential Information of multiple Disclosing Parties.
	2. This DSA does not constitute a release of the Data for the Receiving Party’s discretionary use. Receiving Party must use the Data received or accessed under this DSA only to carry out the purpose and justification of this agreement as set out in section 2, Purpose and Authority for Data Sharing. Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted.
	3. Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

### Security of Data

* 1. Data Protection

The Receiving Party must protect and maintain all Confidential Information gained by reason of this DSA against unauthorized use, access, disclosure, modification or loss. This duty requires the Receiving Party to employ reasonable security measures, which include restricting access to the Confidential Information by:

1. Allowing access only to staff that have an authorized business requirement to view the Confidential Information.
2. Physically securing any computers, documents, or other media containing the Confidential Information.
	1. Data Security Standards

Receiving Party must comply with the Data Security Requirements set out in [Include Exhibit with agency-specific security requirements, if applicable. Consider at least data segregation, transmission, encryption and disposal.] and the Washington OCIO Security Standard No. 141.10. The Security Standard 141.10 is hereby incorporated by reference into this DSA.

* 1. Data Disposition

Upon request or when no longer needed, Confidential Information/Data must be securely disposed of as [Agreed by the parties. Include disposal requirements as part of security requirements, if applicable. Consider methods for paper and electronic information, as well as when it may impossible to immediately destroy data (for example, when complete destruction would require destroying network disks)]*,* except as required to be maintained for compliance with the law or accounting purposes. Receiving Party will provide written certification of disposition upon request using Exhibit \_\_, Certification of Disposal.

### Data Confidentiality and Non-Disclosure

* 1. Data Confidentiality

The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose and justification of this DSA, as set out in Sections 1 and 2 above, except as provided by law.

* 1. Non-Disclosure of Data

The Receiving Party must ensure that all employees or Subcontractors who will have access to the Data described in this DSA (including both employees who will use the Data and IT support staff) are instructed and made aware of the use restrictions and protection requirements of this DSA before gaining access to the Data identified herein. The Receiving Party will also instruct and make any new employee aware of the use restrictions and protection requirements of this DSA before they gain access to the Data.

The Receiving Party will ensure that each Subcontractor who will access the Data signs the [Agency non-disclosure agreement], Exhibit \_\_ hereto or can verify that a substantially equivalent agreement or obligation has been secured. The Receiving Party will retain the signed copy of the *User Agreement on Non-Disclosure of Confidential Information* for a minimum of six years from the date the Subcontractor’s access to the Data ends. The documentation must be available upon request.

* 1. Penalties for Unauthorized Disclosure of Data

State and federal laws may prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines.

The Receiving Party accepts full responsibility and liability for any noncompliance by itself, its employees, and its Subcontractors with these laws and any violations of the DSA.

### Public Disclosure

* 1. If the Receiving Party receives a public records request under Chapter 42.56 RCW for any records containing Data subject to this DSA, Receiving Party agrees to notify the Disclosing Party’s Public Disclosure Officer within five (5) business days and to follow the procedure set out in this section before disclosing any records. [Provide contact info for public disclosure officers.]
	2. To the extent consistent with chapter 42.56 RCW, the Receiving Party shall maintain the confidentiality of all such information marked by the Disclosing Party as Confidential Information. If a public disclosure request is made to view Disclosing Party’s Confidential Information, Receiving Party will notify Disclosing Party of the request and of the date that such records will be released to the requester unless Disclosing Party obtains a court order from a court of competent jurisdiction enjoining that disclosure. If Disclosing Party fails to obtain the court order enjoining disclosure, Receiving Party will release the requested information on the date specified.

### Data Shared with Subcontractors

If Data access is to be provided to a Subcontractor under this DSA, the Receiving Party must include all of the Data constraints, conditions and requirements set forth in this DSA in any such Subcontract, or verify that a substantially equivalent term is included. In no event will the existence of the Subcontract operate to release or reduce the liability of the Receiving Party for any breach in the performance of the Receiving Party’s responsibilities.

### Data Breach Notification

The Breach of Data shared under this DSA must be reported to the appropriate [Privacy Officer, if applicable, otherwise include appropriate agency contact] within one (1) business day of discovery. The [Privacy Officers, if applicable, otherwise appropriate agency contacts] for each of the Parties is listed below. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by applicable law or reasonably requested in order to meet its regulatory obligations.

* [List contact information by party]

### Amendments and Alterations

This DSA, or any term or condition, may be modified only by a written amendment signed by all parties. Only personnel authorized to bind each of the parties will sign an amendment.

### Assignment

The Receiving Party will not assign rights or obligations derived from this DSA to a third party.

### Dispute Resolution

* 1. [Include agency preferred dispute resolution process, which may vary significantly depending on the parties involved]
	2. The Parties agree that, the existence of a dispute notwithstanding, the Parties will continue without delay to carry out all respective responsibilities under this Agreement that are not affected by the dispute.

### Entire Agreement

This DSA, including all documents attached to or incorporated by reference, contains all the terms and conditions agreed upon by the parties. No other understandings or representations, oral or otherwise, regarding the subject matter of this DSA, will be deemed to exist or bind the parties.

### Governing Law and Venue

This DSA is governed by, and will be construed and enforced in accordance with, the laws of the State of Washington. In the event of a lawsuit involving this DSA, jurisdiction is proper only in the Superior Court of Washington, and venue is proper only in Thurston County, Washington.

### Incorporated Documents and Order of Precedence

* 1. Each of the documents listed below is, by this reference, incorporated into this DSA as though fully set forth herein.
1. [Include applicable exhibits]
2. OCIO Security Standard No. 141.10, *Securing Information Technology Assets Standards: Data Security* (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.)
	1. In the event of any inconsistency in this DSA, the inconsistency will be resolved in the following order of precedence:
3. Applicable federal and state statutes, laws, and regulations;
4. Sections of this DSA;
5. Attachments, Exhibits and Schedules to this DSA.

### Inspection

No more than once per quarter during the term of this DSA and for six (6) years following termination or expiration of this DSA, the Disclosing Party will have the right at reasonable times and upon no less than five (5) business days prior written notice to access the Receiving Party’s records and place of business for the purpose of auditing, and evaluating the Receiving Party’s compliance with this DSA and applicable laws and regulations.

### Legal Notices

Any other notice or demand or other communication required or permitted to be given under this DSA or applicable law will be effective only if it is in writing and signed by the applicable party, properly addressed, and either delivered in person, or by a recognized courier service, or deposited with the United States Postal Service as first-class mail, postage prepaid certified mail, return receipt requested, to the parties at the addresses provided in this section.

1. To [party] at:

[Address of Party]

1. [repeat for each party]

Notices will be effective upon receipt or four (4) Business Days after mailing, whichever is earlier. The notice address and information provided above may be changed by written notice given as provided above.

### Maintenance of Records

All Parties must maintain records related to compliance with this DSA for six (6) years after expiration or termination of this DSA. Each Party will have the right to access those records during that six-year period for purposes of auditing.

### Responsibility

Each Party to this DSA will be responsible for the negligent acts or omissions of its own employees, officers, or agents in the performance of this DSA. No Party will be considered the agent of another Party and no Party assumes any responsibility to another Party for the consequences of any act or omission of any person, firm, or corporation not a party to this DSA.

### Severablility

The provisions of this DSA are severable. If any provision of this DSA is held invalid by any court of competent jurisdiction, that invalidity will not affect the other provisions of this DSA and the invalid provision will be considered modified to conform to the existing law.

### Survival Clauses

The terms and conditions contained in this DSA that by their sense and context are intended to survive the expiration or other termination of this DSA must survive. Surviving terms include, but are not limited to: *Constraints on Use of Data, Security of Data, Data Confidentiality and Non-Disclosure of Data, Data Breach Notification, Dispute Resolution, Inspection, Maintenance of Records, and Responsibility*. [Confirm whether each term is in final agreement, and whether additional terms should be added.]

### Term and Termination

* 1. Term. This DSA will begin on [beginning date] or date of execution, whichever is later, and continue through [ending date], unless terminated sooner as provided in this Section.
	2. Termination for Convenience. Any Party may terminate this DSA for convenience with thirty (30) calendar days’ written notice to the others. However, once Data is accessed by the Receiving Party, this DSA is binding as to the confidentiality, use and disposition of all Data received as a result of access, unless otherwise agreed in writing.
	3. Termination for Cause. Any Disclosing Party may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party, if it has a reasonable basis to believe that the Receiving Party has: (1) failed to perform under any provision of this DSA; (2) violated any law, regulation, rule, or ordinance applicable to this DSA; and/or (3) otherwise breached any provision or condition of this DSA.

Before terminating for default, the Disclosing Party will provide the Receiving Party with written notice of its noncompliance with the DSA and provide the Receiving Party a reasonable opportunity to correct its noncompliance. If the Receiving Party does not correct the noncompliance within the period of time specified in the written notice of noncompliance, the Disclosing Party may then terminate the DSA. The determination of whether or not the Receiving Party corrected the noncompliance will be made by the Disclosing Party, in its sole discretion.

### Waiver

Waiver of any breach or default on any occasion will not be deemed to be a waiver of any subsequent breach or default. Any waiver will not be construed to be a modification of the terms and conditions of this DSA.

### Signatures and Counterparts

The signatures on the cover page indicate agreement between the Parties. The Parties may execute this DSA in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement.

Exhibit \_\_

**Certification of Disposal of Confidential Information**

|  |  |
| --- | --- |
| NAME OF RECEIVING PARTY:       | CONTRACT #:       |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Receiving Party) herby certifies that the data described below, received as a part of the data provided in accordance with the contract listed above have been disposed of.

You certify that you returned or securely destroyed all identified confidential information received from [Disclosing Party], or created, maintained, or received by you on behalf of [Disclosing Party]. You certify that you did not retain any copies of this confidential information.

Description of Information

Date of Destruction or Return:

Method(s) of disposal:

Disposed by:

|  |  |
| --- | --- |
| Signature | Date |
| Printed Name: |  |
| Title: |  |