# Data Share Agreement Sample

Overarching agreement for system access or pre-defined extract

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 data sharing agreement tailored for use when the sharing involves system access or a pre-defined extract that can be described in detail.

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.

###

### Definitions

[Definitions should always be checked after the rest of the DSA is drafted to ensure that appropriate terms are included and to delete the terms below that are not in use in the final DSA]

**[“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.]

**“Authorized User”** means an individual or individuals with an authorized business need to access Confidential Information under this DSA.

**“Breach”** means the acquisition, access, use, or disclosure of Data in a manner not permitted under law, including but not limited to the compromise or potential compromise of Confidential Information 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. For purposes of this DSA, Breach includes any Security Incident.

**“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” or “Personal Information.”

**“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.

**“Permissible Use”** means only those uses authorized in this DSA and as specifically defined herein.

**“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 (including or excluding zip code), telephone numbers, social security numbers, driver’s license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

**“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 the entity that is identified on the cover page of this DSA and is a party 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 the 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.

**“Use”** includes the sharing, employment, application, utilization, examination, or analysis, of Confidential Information within an entity that maintains such information.

### Description of Data to be Shared / Data Licensing Statements

[Use 2.1 for DSAs that involve routine sharing of pre-defined files or as a supplement to system access described in 2.3.]

* 1. Data Licensing Statements are the written statements that define the following, at a minimum:
		1. Identification of the purpose and authority for sharing;
		2. Identification of transmission method and frequency;
		3. Identification of the users or classes of users who will have access; and
		4. Identification of the file layout, including description and data classification.
	2. There must be at least one Data Licensing Statement attached hereto, but more than one Data Licensing Statement may be included or incorporated into this DSA at different times. Each Data Licensing Statement is incorporated into this DSA by using the same Attachment reference letter (A) and then further marking it with sequential identifying numbers (A1, A2, A3).
	3. The Receiving Party may request access to the [system] for up to [#] Authorized Users under this DSA.
		1. The Receiving Party Contract Manager, identified in Section 3.4 must send the request to [appropriate Agency contact].
		2. The Receiving Party must access the system(s) through the State Governmental Network (SGN), or SecureAccessWashington (SAW), or through another method of secure access approved by [Agency] in writing.
		3. Receiving Party Point of Contact. The Receiving Party Point of Contact will be the single source of access requests and the person [Agency] will contact for any follow-up information or to initiate an audit under this DSA. Receiving Party Point of Contact may be changed by written notice to the [appropriate Agency contact], email acceptable, with a copy to [appropriate Agency contacts].

|  |  |
| --- | --- |
| Name and Title |       |
| Address |       |
| Telephone |       |
| Email |       |

* + 1. [Agency] will grant the appropriate access permissions to Receiving Party Authorized Users within 30 calendar days from the date of receipt of a complete and accurate request form. [Agency] will respond within 5 business days of receipt of request form if there is a need for clarification or revisions to any inaccurate or incomplete request form(s).
		2. [Agency] does not allow shared User IDs and passwords for use with Confidential Information or to access systems that contain Confidential Information. Receiving Party must ensure that only Authorized Users access and Use the system(s) in this DSA, use only their own User ID and password to access the system(s), and do not allow employees or others who are not authorized to borrow a User ID or password to access any system(s).
		3. Receiving Party must notify [Agency] within 5 business days whenever an Authorized User who has access to the Data is no longer employed by the Receiving Part or whenever an Authorized User’s duties change such that the user no longer requires access to the Data.
		4. Receiving Party’s access to the systems may be continuously tracked and monitored. [Agency] reserves the right, at any time, to terminate Data access for an individual, conduct audits of system(s) access and use, and to investigate possible violations of this DSA and/or violations of applicable federal and state laws and regulations governing access to Confidential Information.

### 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. Subject to the Terms and Conditions of this DSA, [Agency] hereby grants Receiving Party a limited license for the access and Permissible Use of Data. This grant of access may not be deemed as providing Receiving Party with ownership rights to the Data. The Data being shared/accessed is owned and belongs to [Agency].
	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 DSA as set out in the Data Licensing Statement(s). Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted without [Agency’s] prior written consent.
	3. This DSA does not constitute a release for Receiving Party to share the Data with any third parties, including Subcontractors, even if for authorized use(s) under this DSA, without the third party release being approved by [Agency] and identified in the Data Licensing Statement(s).
	4. Derivative Data Product Review and Release Process. All reports derived from Data shared under this DSA, produced by Receiving Party that are created with the intention of being published for or shared with external customers (Data Product(s)) must be sent to [Agency] for review of usability, data sensitivity, data accuracy, completeness, and consistency with [Agency] standards prior to disclosure. This review will be conducted and response of suggestions, concerns, or approval provided to Receiving Party within 10 business days. [Include reference and/or incorporate any specific agency standards that must be met, such as small numbers guidelines.]
	5. Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.

### Data Modification(s)

Any modification to the Purpose, Justification, Description of Data to be Shared/Data Licensing Statement(s), and Permissible Use, is required to be approved by [Agency] and documented in an Amendment to the DSA.

### 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 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, justification, and Permissible Use of this DSA, as set out in the attached Data Licensing Statement(s), except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Data.

* 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

[Use for other Public Agencies]

9.1. 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.]

9.2. 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.

[Use for all other Receiving Parties]

Receiving Party acknowledges that [Agency] is subject to the Public Records Act (Chapter 42.56 RCW). This DSA will be a “public record” as defined in Chapter 42.56 RCW. Any documents submitted to [Agency] by Receiving Party may also be construed as “public records” and therefore subject to public disclosure.

### 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.

### Audit

10.1. At [Agency’s] request or in accordance with OCIO 141.10, Receiving Party shall obtain audits covering Data Security and Permissible Use. Receiving Party may cover both the Permissible Use and the Data Security Requirements under the same audit, or under separate audits. The term, “independent third-party” as referenced in this section means an outside auditor that is an independent auditing firm.

10.2. Data Security audits must demonstrate compliance with Data Security standards adopted by the OCIO, and as set forth in [Agency security standards]. At a minimum, audit(s) must determine whether Data Security policies, procedures, and controls are in place to ensure compliance with all Data Security Requirements set forth herein and as required by state and federal law.

10.3. Permissible Use Audits must determine whether Permissible Use policies, procedures, and controls are in place to ensure compliance with all Permissible Use requirements in this DSA.

10.4. [Agency] may monitor, investigate, and audit the use of Personal Information received by Receiving Party through this DSA. The monitoring and investigating may include the act of introducing data containing unique but false information (commonly referred to as “salting” or “seeding”) that can be used later to identify inappropriate use or disclosure of Data.

10.5. During the term of this DSA and for six (6) years following termination or expiration of this DSA, [Agency] 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.

### Data Breach Notification

11.1. The compromise or potential compromise of Confidential Information 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 must be reported to the [Agency privacy contact] within one (1) business day of discovery.

11.2. 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 19.255.010, RCW 42.56.590, or any other applicable breach notification law or rule.

E. Any other information [Agency] reasonably requests.

11.3. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or [Agency].

11.4. If notification to individuals must, in the sole judgement of [Agency], must be made Receiving Party will further cooperate and facilitate notification to required parties, which may include notification to affected individuals, the media, the Attorney General’s Office, or other authorities based on applicable law.

At [Agency’s] discretion, Receiving Party may be required to directly fulfill notification requirements, or if [Agency] elects to perform the notifications, Receiving Party must reimburse [Agency] for all associated costs.

11.5. Receiving Party is responsible for all costs incurred in connection with a security incident, privacy breach, or potential compromise of Data, including:

A. Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;

B. Notification and call center services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identify theft assistance; and

C. Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

11.6. Any breach of this section may result in termination of the DSA and the demand for return or disposition of all [Agency] Data.

11.7. Receiving Party’s obligations regarding breach notification survive the termination of this DSA and continue for as long as Receiving Party maintains the Data and for any Breach or potential Breach, at any time.

### Offshoring

Receiving Party must maintain all hardcopies containing Confidential Information only from locations in the United States.

Receiving Party may not directly or indirectly (including through Subcontractors) transport any Data, hardcopy or electronic, outside the United States unless it has advance written approval from [Agency].

### 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 without the prior, written consent of [Agency] and the written assumption of the Receiving Party’s obligations by the 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.

### Insurance

20.1. The Receiving Party certifies that it is self-insured, is a member of a risk pool, or maintains the types and amounts of insurance identified below and will provide certificates of insurance to that effect to [Agency] upon request.

20.2. Required Insurance or Self-Insured Equivalent

a. Commercial General Liability Insurance (CGL) covering the risks of bodily injury (including death), property damage, and contractual liability, with a limit of not less than [minimum per occurrence and aggregate].

b. Privacy Breach Response Coverage. For the term of this DSA and 3 years following its termination or expiration, Receiving Party must maintain insurance to cover costs incurred in connection with a security incident, privacy Breach, or potential compromise of Data, including:

i. Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;

ii. Notification and call center services for individuals affected by a security incident, or privacy Breach;

iii. Breach resolution and mitigation services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identity theft assistance; and

iv. Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

c. If any of the required policies provide coverage on a claims-made basis:

i. The retroactive date must be shown and must be before the date of the DSA or of the beginning of DSA work.

ii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the DSA effective date, the Receiving Party must purchase “extended reporting” coverage for a minimum of 3 years after completion of DSA work.

The State of Washington, including but not limited to [Agency], must be named as additional insureds.

In the event of cancellation, non-renewal, revocation or other termination of any insurance coverage required by this DSA, Receiving Party must provide written notice of such to [Agency] within one (1) Business Day of Receiving Party’s receipt of such notice.

By requiring insurance herein, [Agency] does not represent that coverage and limits will be adequate to protect Receiving Party. Such coverage and limits will not limit Receiving Party’s liability under the indemnities and reimbursements granted to [Agency] in this DSA.

### 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. [Agency] or its designee will have the right to access those records during that six-year period for purposes of auditing.

### Responsibility

[Agency] and the Receiving Party will each be responsible for their own acts and omissions and for the acts and omissions of their agents and employees. Receiving Party must defend, protect, and save [Agency] harmless from and against any loss and all claims, settlements, judgments, costs, penalties, and expenses, including reasonable attorney fees, arising from any intentional or negligent acts or omissions while performing under the terms of this DSA. Each party agrees to promptly notify the other party in writing of any claim and provide the other party the opportunity to defend and settle the claim.

### 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. Either Party may terminate this DSA for convenience with thirty (30) calendar days’ written notice to the other. 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. [Agency] 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, [Agency] 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, [Agency] may then terminate the DSA. The determination of whether or not the Receiving Party corrected the noncompliance will be made by [Agency], 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.

**Attachment A1: Data Licensing Statement**

1. **Background**

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

1. **Justification 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.]

1. **Purpose / Use / Description of Data**

The purpose of this DSA is to provide terms and conditions under which [Agency] will allow the restricted use of its Data to the Receiving Party, and under which the Receiving Party may receive and use the Data. This DSA ensures that Data is provided, protected, and used only for purposes authorized by state and federal law governing such Data use.

The scope of this DSA only provides the Receiving Party with access and Permissible Use of Data; it does not establish an agency relationship or independent contractor relationship between [Agency] and the Receiving Party.

[Explain the data to be shared, and the Use of the data, flow of the data, etc.]

Permissible Use: Receiving Party may only use the Data for the purposes of [describe permissible use].

File Layout: The Parties will exchange Data using the mutually agreed upon file layouts below. The Parties may edit and/or change the *File Layout* as considered necessary.

Method of Access/Transfer: [Describe transmission method and any applicable processes].

Frequency of Data Delivery: [Frequency].

[Example columns for data description below]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Element Name | Short Description | Length | Type | Data Descriptions and Usages |
|  |  |  |  |  |

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 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: |  |